UNCLASSIFIED

Strategic Early Warning for Criminal Intelligence

Theoretical Framework and Sentinel Methodology

A paper prepared by Criminal Intelligence Service Canada (CISC) for the Canadian intelligence community

SCRC
CISC

CRIMINAL INTELLIGENCE SERVICE CANADA

Central Bureau, Ottawa

NOTE ON COPYRIGHT AND USAGE:

Table of contents

List of Figures

INTRODUCTION

The professional craft of intelligence analysis is continually evolving. Nowhere has this evolution been more pronounced in recent years than in the domain of law enforcement. The emergence of *intelligence-led policing* as both an organizational doctrine and fundamental practice has profoundly altered the way law enforcement agencies think and operate in the 21st century. There is a growing recognition in the law enforcement community that, to be truly proactive, police must be prepared to act against emerging and future threats—if we wait until a threat becomes full-blown, then we have failed the communities we serve to protect. In order to be proactive, therefore, law enforcement must be armed not only with the best current intelligence, but with foresight on the threat environment of tomorrow. With adequate forewarning of future threats, law enforcement decision-makers are in a better position to develop and implement proactive planning measures, and front-line officers are better-equipped to recognize and deal with the earliest indications of a threat's emergence. For both leaders and operators, warning is a tool to help avert the condition of being surprised by our principal adversary: organized crime.

In an effort to provide the law enforcement community with advanced warning of emerging and future threats, CISC Central Bureau embarked on a project in 2004 to develop a Strategic Early Warning System for organized and serious crime (SEWS). Built upon well-established concepts and principles from such sectors as national defence and public health, and adapting methodological practices from the social sciences, the SEWS project seeks to provide guidance and insight through highly focused criminal forecasts.

Structurally divided into three main parts, this paper provides an overview of the theoretical framework upon which this project was developed, followed by a thorough explanation of the methodological process by which warning is produced and communicated through the *Sentinel* product line. The first part looks at principles and practices of indications and warning (I&W) analysis, outlining its central premise, articulating its key concepts and distinguishing it from other forms of intelligence analysis. The second part is devoted to explaining the SEWS methodology. Beginning with a brief overview of the entire process, this section then discusses in detail the process for developing the *Sentinel WatchList* and the *Sentinel Assessment*, followed by a discussion on the key principles and methods of communicating warning to the client. The third and final part highlights some of the challenges and limitations of a strategic early warning system for organized and serious crime.

I. THEORETICAL FRAMEWORK

Surprise is an enduring feature of human conflict. The competitive advantage afforded by confounding an adversary as to one's true capabilities and intentions means that there are powerful—if not natural—incentives to deny, confuse, and deceive one's enemy wherever and whenever suitable. This fact alone ultimately explains why intelligence exists as a discipline and a profession—if everyone was always completely forthcoming about their plans and capabilities, there would be little need for spies, spy satellites, and intelligence analysts. However, by ignoring or misinterpreting the indications of our enemies' intentions, we can—and often do—deceive ourselves. The history of strategic military surprise reveals that surprise attacks are rarely ever pure 'bolts from the blue'—in almost every case, there has been a host of warning signals leading up to the attack that, had the defender interpreted them correctly, could have averted or, at least, mitigated disaster. In many such cases, surprise was the result of an unwillingness to let go of erroneous strategic preconceptions in the face of the changing tactical situation observed on the ground. Military indications and warning (I&W) analysis is now a well-established component of most professional militaries for this very reason.

Prominent examples of strategic surprise

- Pearl Harbor – 1941
- Yom Kippur War – 1973
- Iranian revolution – 1979
- Hezbollah bombings in Beirut – 1983
- Al Qaeda terrorist attacks in US – 2001

The events of September 11, 2001 only served to underscore the centrality of the warning function for intelligence. **The central premise behind I&W analysis is that events and phenomena do not occur in a vacuum; they affect, and are affected by, various forces and conditions in both the national and international environment, some of which are directly or indirectly observable.** These indications, interpreted in a proper context, can help us warn of an emerging or future threat. With strategic early warning, appropriate action can be taken to anticipate and deal with a threat before it becomes unmanageable.

A. The Warning Concept and Function

It would be appropriate here to define what we mean by *warning* in this context. Cynthia Grabo, a veteran US Defense Intelligence Agency (DIA) warning analyst (ret.), characterizes warning as **"an intangible, a theory, a deduction, a perception, a belief. It is the product of reasoning or of logic, a hypothesis whose validity can neither be confirmed nor refuted until it is too late."**[1] Warning should not be confused with facts or information. For instance, to note that the enemy is mobilizing its forces is a fact or a piece of information; to conclude from this and other indications that the enemy intends and is preparing to attack is a warning. Warning is the product of an intelligence judgement on the level of threat and risk posed by a particular enemy or scenario. Most importantly, however, **warning must be communicated**; an analytical judgement only becomes warning when it is communicated and understood as such by the receiver. As Grabo points out, "warning that exists only in the mind of the analyst is useless."[2]

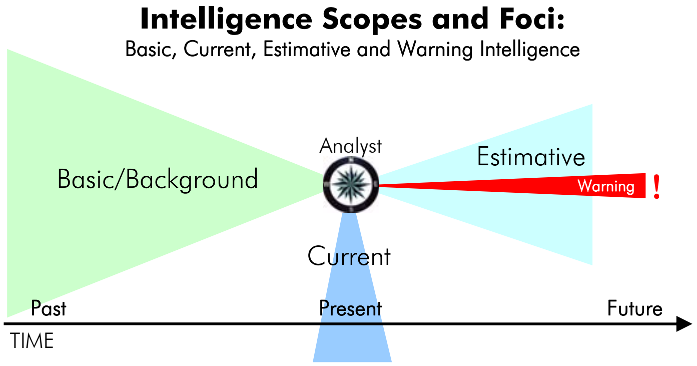
Intelligence Scopes and Foci:
Basic, Current, Estimative and Warning Intelligence
Basic/Background
Analyst
Estimative
Warning
!
Current
Past
Present
Future
TIME

Figure 1 – Distinguishing four types of intelligence by scope and focus

We can distinguish warning analysis from other forms of intelligence analysis by its scope, principal client, and function. In terms of scope, strategic warning is principally focused on the future. In contrast to basic intelligence or current intelligence, each of which seeks to accurately describe past and present realities, warning intelligence is speculative and forward-looking, aiming to characterize a future threat. Although strategic warning analysis is a type of estimative intelligence, I&W is unique in terms of the scope of the question it seeks to address. Whereas estimative intelligence seeks to broadly address the question of a threat's future or that of the threat environment, strategic warning analysis is concerned with answering a highly specific question about the nature of a particular threat: for instance, 'does country *x* have the intention and capability to invade country *y*'. In contrast to most intelligence problems, warning questions can often be answered with a qualified 'yes' or 'no' answer: is there, or is there not, cause for alarm. This narrow, foreword-looking focus makes strategic warning intelligence particularly suited for consumption by senior decision- and policy-makers. Thus, whereas basic and current intelligence are primarily geared towards an operational support function, strategic warning is more tailored to those in a position to direct operational resources on a strategic level.

Current Intelligence	Day-to-day events to keep consumers apprised of new developments.
Estimative Intelligence	Projects forward using known facts, analysis and predictions based upon both, as well as what may not be known.
Warning Intelligence	Communicates danger strongly inherent to interests in a time, form and fashion to enable a decision to be made.

Figure 2 – Warning intelligence distinguished from current and estimative intelligence.[3]

The strategic warning function serves a straightforward but vital purpose: to avert *strategic surprise*—a condition caused when a defence system has failed due to a misconception surrounding *the nature* of a particular enemy or threat. This can be distinguished from tactical surprise, which stems more from a failure to anticipate specific operational realities rather than broader strategic capabilities and intentions. For instance, being attacked by a supposed ally would be a case of strategic surprise—the nature of the enemy was drastically misunderstood. On the other hand, to err in the presumed mode or timing of an anticipated attack would constitute a tactical surprise—the enemy was appropriately understood but the operational attack details were not. Strategic surprise can be averted, then, by providing leaders with timely and convincing warning of an enemy's intention and capacity to threaten the nation's security interests. Without the broader threat context illuminated by strategic warning, tactical warning is severely handicapped, rendering national defences more or less blind up until the last minute.

Figure 3 – By way of metaphor, strategic warning analysis attempts to glean the image on the box of the jigsaw puzzle well in advance in order to make sense of the individual pieces as they are discovered.

b. Indicators, Indications and Warning

I&W analysis is inherently paranoid; more than any other type of intelligence analysis, it operates on the presumption of surprise, and is intrinsically suspicious of widely held beliefs and assumptions about the enemy. This is for good reason: the history of strategic surprise teaches us that bias is the dark side of overwhelming consensus; when a prevailing opinion becomes so accepted and unchallenged that it is equated with 'common sense', the risk of strategic surprise is at its zenith. I&W analysis consciously avoids hegemonic thinking by focusing on the hypothetical. Instead of starting with the question, "What is likely to happen with *x* ?", I&W begins with the hypothetical question, "If country *x* was planning to attack, what behaviours and conditions would we expect to see?" **The starting point for analysis therefore does not rely on a presumption on the likelihood of an occurrence**—if it did, many inquiries would never move beyond this point because of the impact of preconceptions and cognitive biases on threat perceptions. Instead, it begins with the presumption that a threat potential exists in order to develop an *indicator list*, which becomes a key mechanism by which we evaluate a threat potential.

Indicators are just what their name implies: conditions that, if observed, could be indicative of a threat's emergence or its potential to emerge. Major military operations, for instance, often present a host of indicators that could provide a window to intent. As Carl von Clausewitz notes in *On War,* "The preparations for a War usually occupy several months; the assembly of an Army at its principal positions requires generally the formation of depots and magazines, and long marches, the object of which can be guessed soon enough."[4] On their own, an indicator may appear relatively benign, or could be indicative of any number of possible scenarios. However, when a range of indicators are taken together, ambiguity is reduced and a clearer picture begins to form as to what the enemy might be up to. Specific indicators, then, are always developed and interpreted as parts of a whole: the complete indicator list. Military I&W units maintain indicator lists for a wide range of possible scenarios, and are continuously scanning the global environment for possible *indications* (observed indicators) of a threat. Indicator lists are the product of an in-depth research effort and, ideally, produced by—or in consultation with—experts in the relevant subjects or regions concerned. The task of the warning analyst is to incorporate an understanding of the enemy's culture, history, and politico-military doctrines into his/her interpretation of the indications and the broader geopolitical context. If a threat is perceived, the warning mechanism is activated and the relevant commanders and political leaders are alerted.

C. Adapting I&W Analysis for Criminal Intelligence

Adapting practices and principles developed for the military for use in criminal intelligence first requires us to address and reconcile the important differences between the two domains as they relate to the warning mission. Most of the differences stem from the contrasting natures of their adversaries. Military I&W analysis is designed to help anticipate the moves of a known state adversary. The nation state—with fixed map coordinates, national economy and infrastructure, and clear political and military leadership echelons—presents a stunning contrast to the fluid, mobile, and networked entities that make up much organized crime. Unlike most nations, many organized crime groups have neither strategic vision nor established doctrine that could assist an outsider to anticipate their moves. In some cases, then, we may be faced with the task of warning of potential future threats that the organized crime groups themselves may not have yet fully considered. Moreover, in many cases, the strategic threats that concern criminal intelligence are not specific entities at all, but rather criminal *phenomena*, such as new criminal applications of technology, or the expansion of an illicit commodity. As a result, warning analysis for criminal intelligence must contend with a far greater number of variables and a conceivably limitless array of possible outcomes.

Notwithstanding these and other differences, the principle aim and method of military indications and warning analysis has been successfully adapted for use in other domains, most notably in the public health and corporate sectors. Regardless of whether the issue in question is the potential for a military invasion, an influenza pandemic, a hostile corporate takeover, or the emergence of a new criminal market, the central premise behind I&W analysis holds true: that **crisis situations are often the culmination of a series of events and conditions, some of which will generate detectable signals or warning indications that, if correctly pieced together, can portend the coming calamity.** Our 2004 strategic early warning feasibility study demonstrated that this premise is applicable to events and conditions in the criminal underworld. This study, carried out in collaboration with researchers from the Centre for Security and Defence Studies at Carleton University, sought to understand the apparent intelligence failure surrounding the unexpected arrival and establishment of Russian organized crime in the west in the 1990s. The study concluded that observable and potentially predictable linkages do exist between domestic and international indicators on the one hand, and criminal activity in Canada and abroad on the other. In other words, this particular 'intelligence failure' was not inevitable; a sound I&W approach could conceivably have led to early warning and response.

II. Strategic Early Warning Methodology

A. Process Overview

The process for the development of warning intelligence mirrors the traditional intelligence cycle with one key exception: its inception. The traditional cycle begins with a managerial or executive directive informed by what the intelligence decision-making echelon believes are its priorities. For instance, the process for developing an intelligence assessment on the *Hells Angels* would normally begin at the planning and direction stage, where decision-makers would task intelligence officers and analysts with the project based on a decision that Outlaw Motorcycle Gangs (OMGs) are an intelligence priority. Planning and direction is therefore a critical stage in the traditional intelligence cycle, as it ensures that intelligence resources are best utilized to address intelligence priorities. This stage, however, assumes a significantly different form and function in the warning process. In contrast to a focus on known threats, strategic early warning is, by definition, concerned with the unknown or

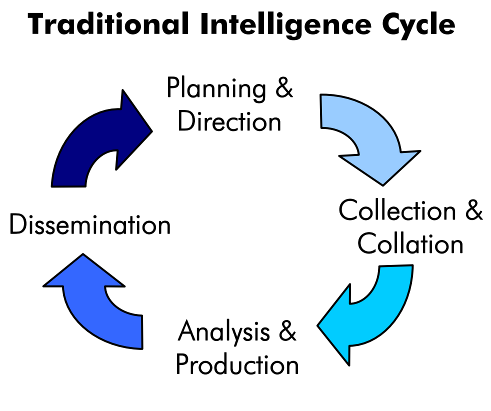

Figure 4 – The traditional intelligence cycle

unexpected dangers over the horizon—that is, that which has *not* yet been deemed a priority issue, or perhaps even contemplated by the law enforcement community. Warning analysis, then, does not have the benefit of knowing one's enemy, but is rather confronted with an array of possible enemies limited, in theory, only by the informed intuition of the individual analyst.

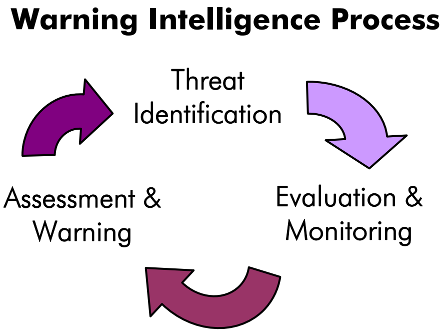

Figure 5 – The warning intelligence process

Given that a SEW assessment will rarely be initiated by a top-down directive, a threat identification and selection mechanism must be built directly into the process. SEW, in contrast, is a case of bottom-up intelligence—the process is initiated by the analysts and the finished intelligence is moved upward to senior executives. Rather than beginning with a known target, the SEW process begins with the search for a target. This will usually take the form of an environmental scan—a continuous process of monitoring various open- and closed-source data streams. This broad scan is virtually boundless in the scope and depth of coverage possible; the analyst must cast an exceptionally wide collection net and, consequently, must sift through a significant amount and range of information, the vast majority of which will not be directly relevant to any eventual product. Some of the key sources of information consulted during the environmental scan include: foreign broadcast media; domestic news; grey literature; academic periodicals; other intelligence assessments; closed-source databases; internet websites; on-line discussion forums and web-logs; environmental scans prepared by different agencies; and, importantly, other analysts and investigators.

The environmental scan should glean possible threat issues for consideration. The review process by which threat issues are evaluated and selected for further analysis is discussed in greater detail below. Once topic candidates have been identified and selected, they are added to the *Sentinel WatchList*, where they then undergo further research and analysis. Throughout this scan, SEW analysts are specifically—though not exclusively—looking for what is new or unusual. The key questions being addressed for each possible threat scenario are: 1) what is the likelihood that the scenario will occur and what is its estimated timeframe; and, 2) what impact would potentially be felt if the threat scenario were to occur.

When the assessments of likelihood and impact potential are adequately answered, a decision can then be made as to whether or not warning is necessary. If not, the issue remains on the *WatchList* for continued monitoring and re-evaluation. If warning is deemed necessary, the topic enters the *Sentinel Assessment* stage, which produces the primary mechanism by which warning is delivered to the intelligence consumer. Throughout the entire cycle, the environmental scanning process never ceases, and threat scenarios are regularly revisited to evaluate whether an important change has occurred that might require the issuance of a new or revised warning. In some cases, further research on an issue may reveal that, while no warning is necessary, there is a need for a dedicated assessment on the topic. In such cases, the issue may, for instance, instead be developed into an estimative intelligence assessment, known as a CISC *Strategic Intelligence Brief*, or perhaps a more comprehensive threat assessment.

The flow chart below (Figure 6) illustrates the SEW process—from threat perception, to evaluation and monitoring, to assessment and warning.[5] As the chart depicts, the law enforcement community is not simply the end-point of this process, but also feeds into both the threat perception and the *WatchList* stages. This reflects the important role played by members of the law enforcement community in offering insight into new possible future threat scenarios, as well as supplying much of the indicator data (indications) for existing *WatchList* and *Sentinel* topics.

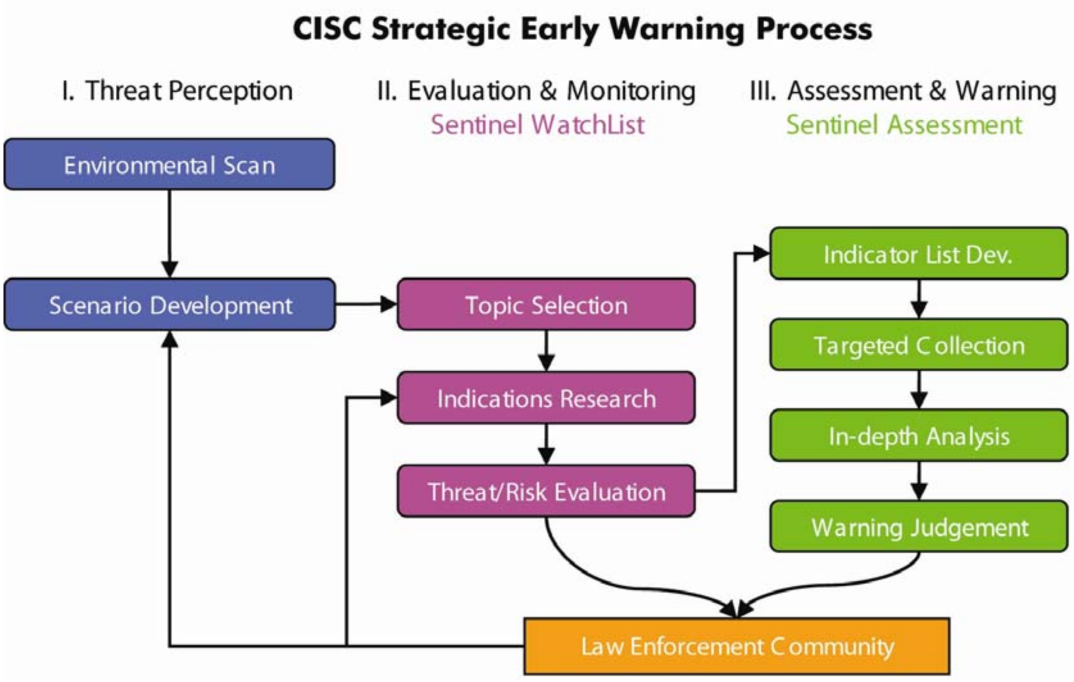

Figure 6 – Flow chart illustrating the CISC SEW process

Expressed another way, the relationship between the *Sentinel* products at each stage is reflected below:

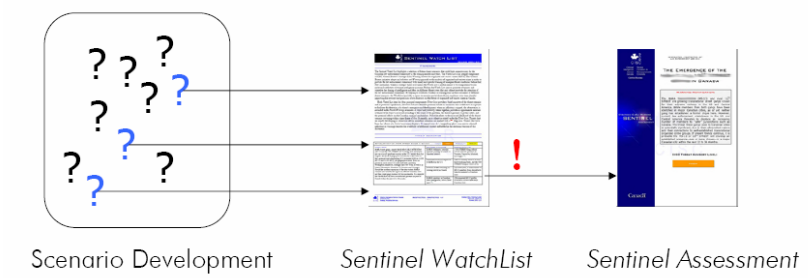

Figure 7 – Life-cycle of threat scenarios through the SEW process

B. THE SENTINEL WATCHLIST

The *Sentinel WatchList* functions as both an analytical tool and an early warning reporting mechanism. In the former function, the *WatchList* serves as a topic clearinghouse for *Sentinel Assessment*s, allowing the warning analyst to record and observe changes over time for a range of possible threat issues, thereby making it easier to see when a particular topic meets the threshold for a *Sentinel Assessment*. The *WatchList* is also a mechanism for promoting awareness and stimulating the sharing of intelligence and ideas on different threat issues that may otherwise evade the attention of the law enforcement community. The *WatchList* ensures wide exposure to potential threat scenarios that may lack sufficient research development to be the subject of a full assessment. In so doing, the *WatchList* acts as an incubator where information and understanding on potential threats can grow and develop. It should be emphasized that the *WatchList* is not intended as a means to identify new law enforcement priorities—its function does not go beyond the promotion of awareness and discussion of potential emerging and future threats.

Figure 8 – The scope of the topic identification process is global; events and conditions around the world are evaluated in the context of the Canadian situation to develop potential threat scenarios that could have an impact on us now or in the future.

i. Topic identification process—The identification of threat scenarios for inclusion in the *WatchList* begins with an all-source, global environmental scan. From this scan, the warning analyst identifies conditions, phenomena, actors or groups—in Canada or abroad—that could conceivably have implications for Canadian law enforcement in the coming months and years. This positing on potential future threats is an inherently subjective exercise. Scenario development is based largely on what could be termed imaginative threat perception, or, in other words, educated guesswork—the process must therefore be unrestricted to enable warning analysts to think freely and creatively about the potential threats of tomorrow. Once a scenario is developed, the warning analysts collectively make a preliminary estimate on the likelihood of the scenario's occurrence on a five-level scale: nil, low, medium, high, and near-certain. The third step involves a collective estimate on the potential impact the scenario could have if it were to occur.

From this informal, collaborative review process, scenarios that are deemed plausible and carry conceivably important implications for law enforcement are flagged for more in-depth research and analysis. While group consensus on the likelihood of the threat scenario is not necessary, it is desirable to achieve a consensus on the relative significance of the scenario if it were to occur—assessments of likelihood often change with the arrival of new information or with a change in conditions, and so the importance of likelihood is relegated at this early stage. Other factors for consideration include: whether the scenario could plausibly occur within the coming several years; whether the topic addresses an intelligence gap; whether the topic is already being looked at by the law enforcement community (duplication of effort is avoided); whether the topic would be of interest to law enforcement decision- and policy-makers; whether the topic fits within the agency mandate; whether we have access to the necessary expertise and information to effectively examine the topic. **The *WatchList* is concerned with specific threat scenarios rather than broad possible futures.** As such, *WatchList* topics, though focused on future events and conditions, should be grounded in the present reality; the present is the point of departure for analyzing and forecasting an emerging or future threat.

It is important to underscore that these early estimates of likelihood and impact are cursory—based more on logical reasoning than on an appraisal of the available evidence. This is because the topic identification process precedes targeted collection and rigorous analysis—this process is intended only to flag good topic candidates for further study and to filter out the implausible or insignificant ones. As such, these preliminary likelihood and impact estimates are subject to change as new information enters the analysis.

ii. Initial research—The identification of a potential threat scenario represents the first stage of the *WatchList* process; preparing an issue for inclusion in the *WatchList* requires more focused research. The research phase involves identifying and answering the key questions concerning the particular threat scenario. While these questions will depend largely on the specific scenario under examination, some key questions could include: Is there a precedent for this threat; where has it occurred, and under what conditions; what are the push/pull factors or conditions; would current conditions in Canada conceivably permit or promote the development of the threat here; if the threat could not develop here at the present time, what would need to change for the threat to occur here, and how likely is it that these changes will occur in the coming months and years. Essentially, then, the warning analyst is concerned with identifying the conditions that both enable and cause the emergence of the threat scenario, and evaluating those conditions in light of current and foreseeable conditions in Canada. The research approach taken to address these questions will depend on both the nature of the threat scenario as well as the experience and resourcefulness of the individual warning analyst.

iii. *WatchList* indicators—While all types of intelligence—background (or basic), current, estimative and warning—make use of indicators to inform analytical judgments, warning analysis is distinguished from other methods by the pre-eminence of indicators in the analysis and in the finished product. The *WatchList* not only provides a description of the threat scenario and its potential implications, but also identifies some of the key indicators that are monitored to detect the early signs of a threat's emergence and development. Indicators provide a means to observe changes over both the short and long term, and help signal when it is necessary to revise key judgements, such as assessments of impact and probability. Displaying indicators within the product helps to bridge the tactical with the strategic, enabling intelligence consumers—as well as the information contributors—to see how tactical information informs strategic judgements.

Indicators generally fall under one of two categories: *primary* indicators (or *agency* indicators) and *secondary* indicators (or *structural* indicators). Primary indicators are those directly relating to activities (or *transactions*) of target individuals or groups. An example of a primary indicator in the case of the arrival of a foreign street gang could be the local identification of the gang's graffiti tags, or the arrest of prominent members in a Canadian city. Secondary indicators, on the other hand, constitute the conditions that would either enable (make possible) or promote (make more likely) something to occur. For example, structural indicators of a gang's arrival could include the size of the potential recruiting pool the gang could draw from, or the existence of a power vacuum or market opportunity that could attract the gang and enable it to establish itself locally.

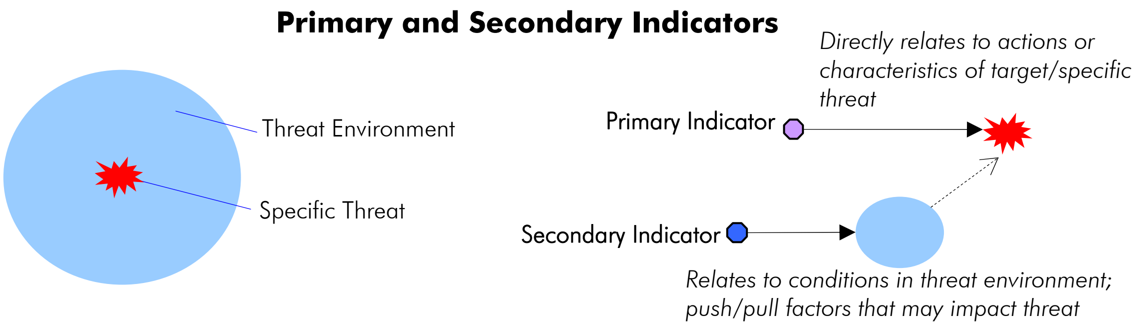
Primary and Secondary Indicators
Threat Environment
Specific Threat
Directly relates to actions or characteristics of target/specific threat
Primary Indicator
Secondary Indicator
Relates to conditions in threat environment; push/pull factors that may impact threat

Figure 9 – The relationship and difference between primary and secondary indicators.

An individual indicator is usually of little value on its own because it could, in fact, be indicative of a number of possible conditions (for instance, the graffiti tag could be the work of a copycat tagger). However, when specific indications are viewed in context with the broader list of indicators, a clearer picture begins to emerge; the number of plausible alternative explanations diminishes as more and better indicators are

Country-based analysis	Group-based analysis	Activity-based analysis
• Conflict history • Governance • Economics • Demographics • Society • Environment • Human development • International involvement • Criminal history • Criminal trends	• Group history • Organization • Core activities • Key members • Alliances / rivalries • Proclivity for violence (see Figure 11 below) • Community base & demographics • Balance of power • Growth potential	• Market dynamics • Competition • Monopoly • Supply chain dynamics • Suppliers • Distribution • Marketing techniques • Demand demographics • Victims • Social impacts

Figure 10 – Indicators can be grouped together according to the condition being assessed. These groupings are referred to as indicator clusters. For instance, multiple indicators can be deployed to assess criminal market competition (such as drug prices and availability, violent rivalry, etc.).

included in the analysis.

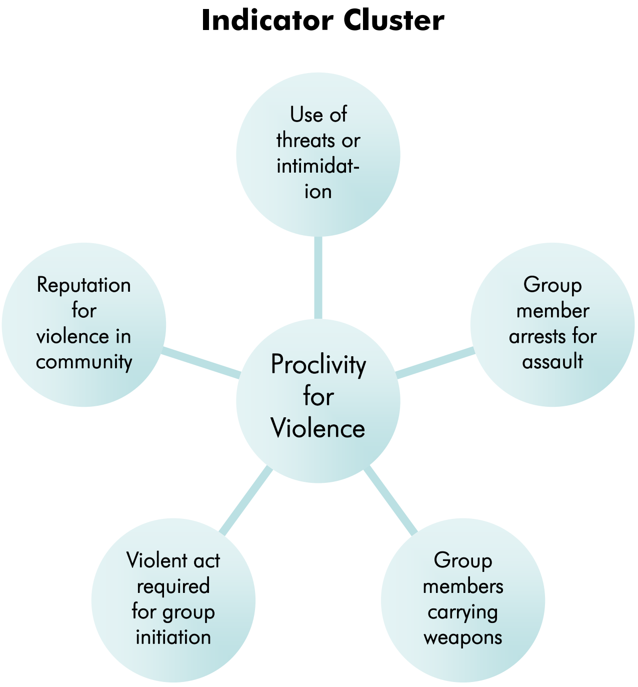
Indicator Cluster
Use of threats or intimidat-ion
Reputation for violence in community
Proclivity for Violence
Group member arrests for assault
Violent act required for group initiation
Group members carrying weapons

Figure 11 – Example of an indicator cluster. Here, five separate indicators are clustered into a single indicator gauging a target group's proclivity for violence.

Indicator development is a fluid process that takes place concurrently with the research phase. An indicator is the product of an analytical inquiry into the conditions that could promote or permit a scenario to occur, and that which we would expect to see if the scenario were to emerge. An analysis of historical precedent is particularly useful in the development of both primary and secondary indicators for the key reason that the past, although not destined to repeat itself, can nevertheless provide important insight into the patterns and trends behind the actions of individuals, groups, or phenomena. In the absence of precedent, the warning analyst must rely on logic and reasoning to identify possible indicators. Some indicators will be fairly obvious. For instance, if the threat scenario in question is the potential for an alliance to form between two gangs, common sense dictates that the existence of strong relations between the gangs would be one primary indicator. However, other indicators will be less obvious, requiring some creativity on the part of the warning analyst. In the same scenario, less obvious indicators could be the existence of a common enemy to the two gangs that is growing in strength and numbers (motive), or the existence of close ties between incarcerated members of both gangs in the prison system (opportunity).

When a scenario concerns specific criminal entities such as individuals or groups, the key task of the warning analyst is to develop indicators pertaining to observable activities (primary indicators). These activities or *transactions* (such as group recruitment, drug trafficking, money laundering, enforcement beatings and retaliatory killings) may emit identifiable *signatures* (such as characteristic tactics, techniques, and procedures) that can be associated to a particular group or actor. Indicator development is essentially about laying tripwires in key nodes or pathways where such transactions and signatures are likely to be detected should a particular threat scenario begin to unfold. As Sullivan notes, "These transactions and signatures can then be observed and matched with patterns of activity that can be expressed as trends and potentials, which can ultimately be assessed in terms of a specific actor's capabilities and intentions."[6] In other words, when transactions and signatures are tracked over time and interpreted in context, they can provide critical insight into the capabilities and intentions of a group or individual.

iv. Building the *WatchList*—The *WatchList* consists of four principal components for each threat scenario under evaluation (Figure 12 illustrates): 1) the *Threat Issue* section provides a brief narrative of the threat scenario and its potential significance; 2) the *Monitored Indicators* column identifies potential trends or conditions that could serve as tripwires to facilitate the detection of a threat's emergence and development; 3) the *Possible Indications* column records key observations that could signal an indicator's presence; and, 4) assessments of *impact* and *probability*, reflected by five-level colour-coded scales, are displayed at the top of each threat scenario. Threats that are rapidly developing or otherwise call for immediate attention are marked with a 🚩 (flag) icon in the *Threat Issue* section. Threats that have been the subject of a *Sentinel Assessment* display a 📄 (report) icon. Finally, a 🔍 (magnifying glass) icon next to selected indicators or indications denotes the availability of additional content embedded in the electronic version of the *WatchList.*

Short Heading of Threat Scenario	Impact: MEDIUM	Probability: HIGH
Threat Issue 🚩	Monitored Indicators	Possible Indications
Brief overview of the threat scenario and its potential implications for Canada, in roughly 150-200 words. This should give a quick overview providing the 'who', 'what', 'where', 'how', and, critically, the 'so what'.	Condition/event that could signal the threat's emergence or development.	Specific observation pertinent to corresponding indicator 🔍
	Indicators are divided by row separators. Between three and five indicators are included for each threat scenario.🔍	Multiple observations are listed, separated by a blank line. All key relevant observations should be listed.
	Indicators for which no observation has been made should still be added, with a note in the adjacent column to indicate that condition has not yet been observed.	*No observed indications*

Figure 12 – *WatchList* item components and basic template

v. Monitoring—A lesson learned from the history of strategic surprise is that potential threats cannot be dismissed and forgotten simply because they are deemed a low risk. Perceptions of risk could be wrong, or conditions could change that increase the likelihood of a threat. Strategic surprises are often products of both pathologies: inaccurate perceptions and a failure to re-evaluate assumptions in light of new or changing realities on the ground. It is for this reason that regular monitoring and re-assessment are integral features of any strategic early warning system. A key function of the *WatchList* is that it enables the tracking of changes to threat indicators over time, thereby facilitating the re-evaluation of threat and risk levels. In addition to scanning for new potential topics, the warning analyst collects information on existing *WatchList* topics during the environmental scan.[7] It is important to emphasize that this monitoring is continual, rather than periodic. New information pertaining to a monitored indicator is incorporated into the *WatchList* either by appending the information to the *possible indications* column as a new observation, or by updating an existing observation (for instance, adding a new city to a list of cities where a gang's graffiti has been documented). The warning analyst indicates where changes have been made by using bolded text and by including dates of new events. Important changes, such as changes in likelihood and impact assessments, are reflected in the *Threat Issue* section with some comment indicating why the threat is more or less serious than initially thought. Threat scenarios that are more slow-moving in their development are shortened and placed in a separate section for unchanged threat scenarios towards the end of the *WatchList*. Should a significant development occur, the scenario is expanded and moved into a separate section for updated threat scenarios.

C. The Sentinel Assessment

The *Sentinel Assessment* ("*Sentinel*") constitutes the primary mechanism by which warning of an emerging or future threat is communicated to the law enforcement community. The *Sentinel* is designed to provide in-depth and focused research, relevant tactical information, and clear strategic judgements in a concise and accessible format for senior law enforcement officials. The principal goal of the *Sentinel* is to raise awareness of a potential threat in order to avert strategic surprise and to enable informed decision-making. It is also hoped that the release of a *Sentinel* will generate discussion within the law enforcement community, promote intelligence sharing on the topic, and raise situational awareness among the eyes and ears of the intelligence community.

i. Criteria for topic selection—Although there is no firm threshold or formula to determine when a *WatchList* item should become the subject of a *Sentinel*, there are certain general considerations that inform when the production of a *Sentinel* is appropriate. One principal consideration is the determination that warning on a particular threat is necessary—whether a need to know exists. The timeliness of the topic is also considered; issues that may require some urgency on the part of the law enforcement community (that is, threats that are potentially imminent) will generally be handled before issues that are some time away from becoming a problem. A third consideration is community interest for coverage on a particular topic. The feasibility of the topic is also considered. Producing a *Sentinel* requires a fair amount of information and intelligence on a given topic. Feasible topics are generally completed within a 4- to 8-week production cycle (assuming that much of the groundwork for the research has already been completed for the *WatchList* entry). Lastly, the impetus for producing a *Sentinel* can stem from a significant change or development relevant to a monitored topic that could alter a previous judgement. For instance, a potential threat scenario initially assessed as low likelihood is affected by a change in border policy that threatens to elevate the likelihood to high.

ii. Articulating the warning problem—Once a topic has been selected for a *Sentinel*, the first step is to outline the specific warning problem that the *Sentinel* seeks to address. This is a critical exercise because the way in which the warning problem is articulated will largely inform how the research effort will be carried out by establishing the parameters and goals of analytical inquiry. The warning problem expresses, in a single sentence, the objective of the present *Sentinel*. For example, the warning problem for a *Sentinel* on the criminal threat to Canada posed by turmoil in Haiti could be expressed as follows: "To evaluate the potential impact and risk of current political events in Haiti on Canada's Haitian-based organized crime groups and their criminal connections to Haiti."

iii. Building upon indicator lists—The indicator list developed for the *WatchList* is only a starting point. When a topic has entered the *Sentinel* research and production stage, it is necessary to further develop the indicator list to inform the judgements of a much more in-depth and comprehensive research endeavour. The *WatchList* outlines only the key primary or agency indicators that point to a threat's potential emergence. In developing the *Sentinel*, it is necessary to also address the secondary or structural indicators, in addition to the primary ones. One of the first steps is to expand the existing indicator list by exhausting the range of possible sites that would likely affect or be affected by the emergence of a threat scenario. As noted earlier, indicators are the product of breaking down a problem into smaller, constituent parts.

The best indicator lists are those that address all the key threat components. If, for instance, the topic is dealing with a commodity such as narcotics or contraband, then indicators may be developed relating to: supply and demand patterns or trends; criminal expertise needed; precursors or materials needed; activity at borders; existing legislation, etc. If dealing with a group, indicators may pertain to: the group's capabilities and intentions; deterrents and incentives; existing balance of power in the criminal underworld; likely responses by other criminal groups and law enforcement; public response; group recruiting potential; community support network; support from other groups; rivalries; change in criminal activities; "chatter" (rumours on the street), etc. By developing a well-defined and comprehensive indicator list, the warning analyst can begin a more targeted and efficient collection effort to evaluate what indications, if any, are present, and thereby come to the best possible judgement on the threat level of a scenario.

iv. Targeted collection—By the time a topic reaches the *Sentinel* development stage, much of the base research has already been completed: threat background; historical precedent; implications; key variables and conditions—these avenues have already been explored for the *WatchList* entry. The developed indicator list should inform new research questions to be addressed. The warning analyst then canvasses the open-source literature, reviews local and international media reporting on the topic, and searches law enforcement intelligence databases for all relevant information. After refining a list of questions or intelligence gaps, the warning analyst then identifies and contacts the individuals he/she needs to consult to address each question. Source interviews are an essential component of the *Sentinel* process as it is through these meetings that warning indications are likely to be revealed to the analyst—investigators, tactical intelligence analysts, medical officers, and other front-line professionals are often the first to detect the earliest indications of a threat's emergence. These interviews also help build source networks that can greatly facilitate the monitoring of a threat issue after a *Sentinel* has been disseminated, and can also aid in the identification of new threat issues.

v. Hypothesis development—Analysis is not so much a stage in the *Sentinel* process but rather an intrinsic feature of it; analytical reasoning begins even before a topic is firmly chosen, during the identification of potential threat issues. However, the analytical process assumes a new momentum when sufficient information has been collected and processed from which to make an informed judgement. The first step is the development of a central research question, which will usually take the form, *will threat scenario x develop to have implications for Canadian law enforcement?* From this research question, a central hypothesis (for instance, *'threat scenario x will occur'*) and its null hypothesis (*'x will not occur'*) are put forward for testing. The specific hypothesis testing procedure will vary case to case, but it essentially involves breaking an issue down into more manageable components. Analytical inquiry assumes two related pathways: identifying the trends/patterns of a particular threat (for instance, how has this threat manifested itself elsewhere); and an analysis of the threat environment for the conditions that would enable or promote the emergence of the threat (are present conditions in Canada favourable to the threat's emergence here).

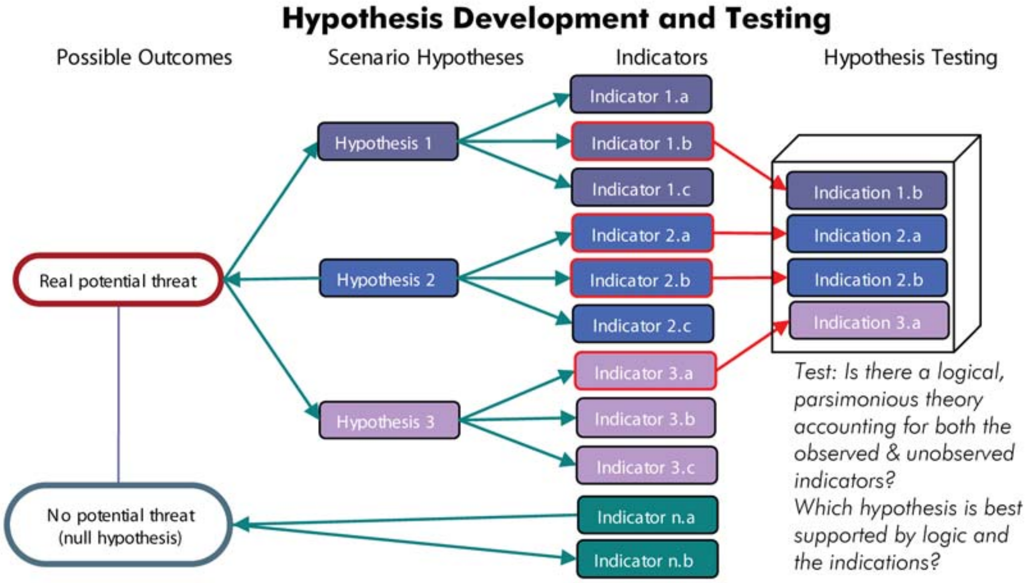

Figure 13 – Diagram illustrating the process by which a central hypothesis is broken down into alternative hypotheses. Key indicators are developed to facilitate hypothesis testing.

vi. Assessing timing—Timing is one of the most difficult variables to accurately gauge in any type of forecasting exercise—one is far more likely to err in assessments of *when* than those of *whether* something will occur. There is a trade-off between precision and accuracy in estimates of timing. Although precise estimates are more useful to the decision-maker (such as those that identify a specific month, week or day when something is expected to occur), they are highly prone to inaccuracy. To provide a meaningful estimate of timing that is more reliable, we offer a timeframe, counted in months, within which we expect the threat scenario, if it is to occur at all, will take place (for instance, 12-24 months). This range is developed through an exercise to identify the earliest and latest points we would expect the scenario to occur in.

This exercise essentially involves beginning with the question, 'would I be surprised if this scenario were to occur within the next 6 months?' If the answer is 'yes', then we consider whether we would be surprised if it were to occur within the next 12 months, and so on until we get a negative response. The point at which we would not be surprised that the scenario would occur becomes our floor (earliest) estimate. This exercise continues from the floor estimate until the response is positive again, which gives us our ceiling (latest) estimate. The resultant floor and ceiling estimates give us our expected timeframe window.

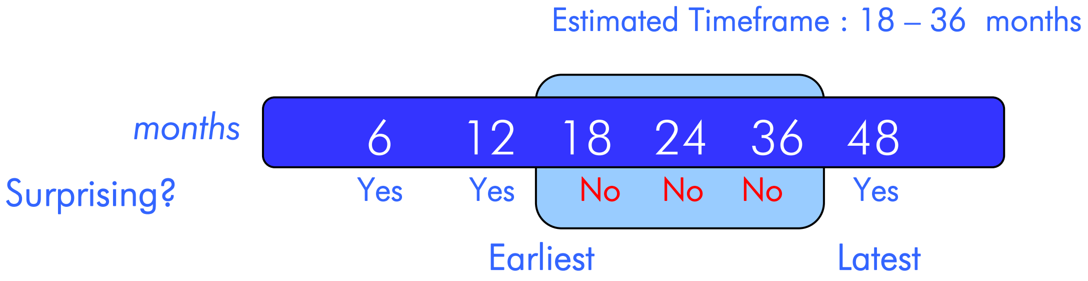

Figure 14 – Illustration of timeframe estimation exercise. In this example, the analyst believes that the threat scenario is most likely to occur within a window of 18 to 36 months from the time of assessment.

In other words, the estimated timeframe becomes the period that would be least surprising to the warning analyst for the emergence of the threat scenario. Clearly, this exercise reflects only an analytical judgement—different analysts presented with the same information could well come up with different outcomes from this exercise. Nevertheless, it is a way for the analyst to develop an approximate estimate of an inherently problematic variable, and communicate this judgement in a way that is meaningful to the intelligence consumer. It should be noted that this exercise is based on the hypothetical premise that the scenario *will* occur—the analyst can estimate a timeframe for an event he/she deems is unlikely to occur. For instance, the timing of a potential event could be assessed at 12 to 18 months while the probability of the event occurring is deemed low. Estimates of timing answer the question, "If this threat scenario were to occur, what would be the most likely timeframe for its emergence?" When the analyst provides an estimate of probability, that estimate relates to the likelihood that the event will occur within the expected timeframe. As such, **the timeframe is estimated independently from probability estimates**.

vii. Assessing probability—The *Sentinel Assessment* and *WatchList* incorporate the same five-level colour-coded scale to reflect the analyst's judgement on the likelihood of the threat scenario's occurrence. Probability level is assigned according to the following key:

CERTAIN	Threat scenario already occurring or its eventual occurrence is "almost certain". Probability at or above 85%
HIGH	The occurrence of the threat scenario is "probable" to "highly likely". Probability at or above 70% but below 85%
MEDIUM	There is a "better than even" to "likely" chance that the threat scenario will occur. Probability above 55% but below 70%
LOW	Scenario occurrence is possible but "improbable"; "little chance" to "about even" chance of occurrence. Probability above 20% but at or below 55%
NIL	Probability of event occurrence is negligible or "highly unlikely". Probability at or below 20%

Figure 15 – Probability key for *Sentinel Assessment* and *WatchList*

The probability key incorporates both qualitative and quantitative measures, providing both statements and corresponding percent ranges to communicate the analyst's probability judgement. The use of a numerical measure in the judgement should not give the false impression that probability is in any way the product of, or related to, statistical practices, formal or otherwise. Both the statements of uncertainty and the percent ranges are simply means to communicate subjective judgement to render it more objectively meaningful.

Much has been written on the difficulties of communicating uncertainty in intelligence assessments. Research from the CIA's Sherman Kent Center, among other institutions, has demonstrated that there is often great variability in readers' interpretations of the most commonly used statements of uncertainty (such as, "probable," "possible," "likely," or "unlikely"). The findings of this body of research suggest that the use of such statements to convey analytical confidence can result in unclear judgements, at best—misinterpretation, at worst. To mitigate this problem we make use of subjective probability estimates in order to provide more clarity to the statements and terms we chose to reflect our confidence in our judgements.

Unlike objective statistical probability, which is based on the objective frequency of a certain condition (for instance, how often a fair coin toss produces a 'heads' result), subjective probability describes an individual's personal judgement about the likelihood of a particular event. Though not based on any precise computation, it is often a reasonable assessment by someone with relevant knowledge. The matrix displayed here[8] shows the relationship between statements of uncertainty and probability estimates, and indicates how our five-level colour-coded scale corresponds to these measures.

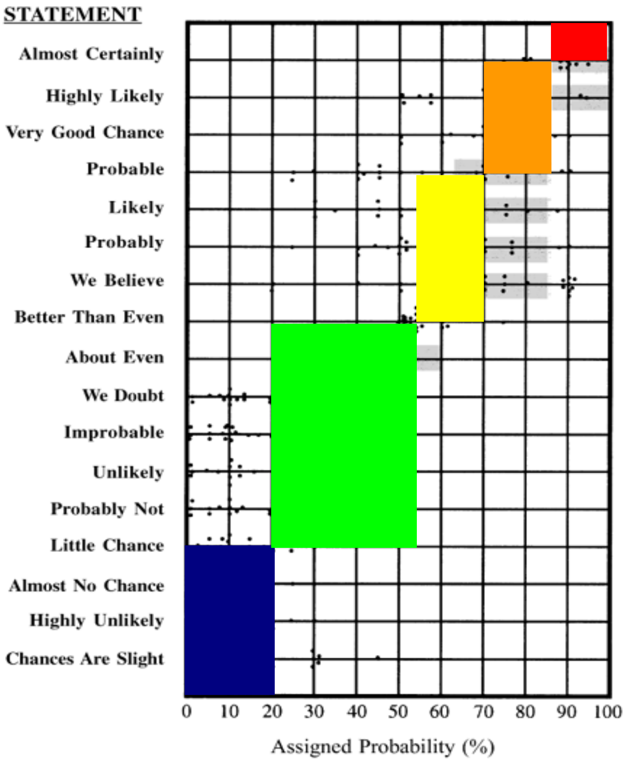

Figure 16 – Matrix showing the five probability levels (Nil, Low, Medium, High, Certain) and their corresponding statements and subjective probability percent ranges. Dots on matrix represent results of a Sherman Kent study on intelligence consumer interpretations of probability statements.

viii. Assessing impact potential—In order to provide intelligence consumers with a sense of the level of threat posed by a particular scenario, the *Sentinel Assessment* and *WatchList* utilize a colour-coded measure of impact potential. Estimating the relative impact of criminal threats is problematic, particularly because impact is a multi-dimensional variable, encompassing a number of different types of implications (social, political, economic, health and safety) on various levels (societal, institutional, group, and individual). As such, the impact key does not attempt to distinguish or weigh different forms of impact, but rather relies on both general and relative descriptions of different impact levels. An emphasis on tangible and visible impact (or "associated costs") reflects the reality that visible criminality has discernable effects on less tangible—but equally important—aspects of Canadian society, such as public fear of victimization. The fact that even localized crime of a highly violent nature can have widespread impact on public life necessitates a general and flexible definition of impact. We measure impact potential according to the following key:

SEVERE	The threat scenario's occurrence would have associated costs that are exceptionally high, clearly visible, and felt across various domains and levels; wide-reaching implications well beyond the area of law enforcement.
HIGH	Considerable and highly visible costs would be incurred with the emergence of the threat scenario; threat would be primarily a law enforcement challenge but would also have a discernable impact on other domains.
MEDIUM	The occurrence of the threat scenario would carry tangible associated costs for Canadian society, some of the effects of which would have significant implications for the Canadian law enforcement community.
LOW	Limited or highly specific and localized costs associated with the emergence of the threat scenario.
NIL	Associated costs would be negligible; no discernable threat.

Figure 17 – Impact Potential key for *Sentinel Assessment* and *WatchList*

ix. Assessing indicator strength—The evidentiary support for indicators will be stronger for some than for others. The *Sentinel Assessment* therefore uses a five-level key to reflect the degree to which the evidence supports the finding that the indicator condition is present. The following key is utilized to reflect only the extent of evidence for a given indicator, and not its intrinsic or relative importance:

EXTREME	Evidence strongly and unambiguously supports finding that condition is present.
HIGH	High degree of corroborated evidence suggesting that condition is present.
MEDIUM	Moderate degree of evidence suggesting presence of condition, some of which is substantiated.
LOW	Evidence of condition is scant and/or inconsistent.
NIL	No evidence to support presence of condition.

Figure 18 – Indicator Strength key for *Sentinel Assessment*

To illustrate how this key is applied in the *Sentinel Assessment*, the following examples depict one primary indicator and one secondary indicator and their corresponding indicator strength levels, each from a different *Sentinel Assessment*.

Primary Indicators	Indicator Strength	Possible Indications
Behavioural changes within *Hells Angels* organization	LOW	Although the *Hells Angels*, its puppet gangs and allies are keeping vigilant about any possible *Bandidos* developments, they do not appear to have altered their behaviour in preparation for conflict with an emergent *Bandidos* problem.

Example 1 – Indicator Strength in a *Sentinel Assessment*

In the above example, the assigned indicator strength of *low* reflects the relative absence of available evidence suggesting that the *Hells Angels* are preparing for a gang war with the *Bandidos*. This rating does not mean that the *Hells Angels* are *not* preparing for, or already engaged in, violence with the rival OMG, but rather that the evidence at present does not indicate that their behaviour has changed in the way we would expect if war was imminent or underway.

Secondary Indicators	Indicator Strength	Possible Indications
Increased volatility of political conditions in Haiti	HIGH	Haiti is verging on the ungovernable; conditions are ripe for a partial balkanization (informal break-up) of the country and criminalization of governmental institutions. The situation is unlikely to change without significant international intervention.

Example 2 – Indicator Strength in a *Sentinel Assessment*

In the second example, the high-level indicator strength reflects a strong degree of corroborated evidence suggesting that political conditions in Haiti are presently tenuous. This should not be interpreted as an analytical judgement that the current political conditions in Haiti pose a *high* threat to Canada or its interests. Indicator strength is not related to estimates of threat or risk, but only reflects the extent to which the evidence supports—or does not support—the presence of a condition.

x. Developing alternate scenarios—In any forecasting exercise, there will rarely be one single scenario consistent with the indications. In most—if not all—cases, a number of alternative plausible scenarios can be constructed from the available facts. Moreover, the probability of particular scenarios will often rely on certain conditions being present or activated, such as how an organized crime group will react to the introduction of a new criminal entity. As such, scenarios can often conceivably play out in a number of different ways. The *Sentinel Assessment* accommodates for this reality by offering the intelligence consumer three potentially different scenarios: the best case; the worst case; and the most likely case—a practice adopted from I&W in the military sector. The advantage of this practice is that it provides intelligence consumers with the spectrum of alternative threat possibilities. For those inclined towards worst case or best case planning, this helps to provide appropriate parameters to guard against unrealistically pessimistic or optimistic thinking. Developing these scenarios is an exercise in alternative hypotheses; the best and worst cases are developed by considering different possibilities that could realistically occur if certain conditions changed, whereas the most likely scenario reflects the primary hypothesis of the *Sentinel Assessment*.

xi. Threat Advisory Level—The final stage in the assessment process for a *Sentinel* involves a determination on the Threat Advisory Level for the specific scenario under analysis. The Threat Advisory Level reflects the analytical judgement outlined in the *judgements and implications* section of the *Sentinel*, and incorporates assessments of probability and impact potential in light of the current indications being observed. While the Threat Advisory Level utilizes the common five-level colour-coded assessment scale, no explanatory key is offered to define the specific meaning behind each threat level (nil, low, medium, high, extreme). Definition of the different levels would be undesirable because the Threat Advisory Level is a holistic and general assessment of overall threat level; the specific considerations that inform this judgement, as well as their relative weighting, are case-specific, thereby making standardized definitions impractical. Threat Advisory Level essentially reflects how loud the alarm is being sounded by the warning analysts.

xii. Production—Production of the *Sentinel* involves adapting the work prepared during the research and analysis stage to the *Sentinel Assessment* product template. The finished draft is then subjected to a series of both formal and informal peer review mechanisms to ensure the accuracy of its information, the soundness of its analysis, and the quality of its presentation. Internally, the draft *Sentinel* is circulated among analysts who have expertise relevant to the issue being examined. Simultaneously, the draft is sent to key officers and analysts in the law enforcement and intelligence communities, most of whom would have been contributors during the research and analysis stage. The external review process is an essential check on the veracity of the information on which the judgements are based, and also ensures that these judgements are consistent with tactical realities. Comments on the draft are returned in writing and/or discussed in person or over the phone. The formal Intelligence Review Board (IRB) brings together analysts, intelligence officers, managers, and the *Sentinel* authors to critically examine the draft *Sentinel*.

Both the internal and external review processes can result in substantial changes being made to the text, which is then revised and re-circulated internally and, if necessary, externally for a second review. The cycle continues until the authors are confident that the warning judgement is sound and its supporting data accurate. The finished product is subsequently translated and professionally printed for national and international dissemination, and submitted electronically to CISC's national intelligence database, the Automated Criminal Intelligence Information System (ACIIS). Client satisfaction surveys are provided to every recipient on the *Sentinel* distribution list.

D. SEW Reporting

"It is an axiom of warning," notes Grabo, "that warning does not exist until it has been conveyed to the policy-maker, and that he must know that he has been warned." The analyst "must find the means to convey what he believes to those who need to know it."[9] Unlike the vast majority of criminal intelligence in Canada, which is geared predominantly towards operational support, strategic warning intelligence is specifically tailored for senior law enforcement decision- and policy-makers. As such, there are important considerations with regards to the principles and methods of reporting for warning intelligence.

i. Consumers of *Sentinel* warning intelligence—Though senior decision- and policy-makers constitute the primary intended audience for strategic warning intelligence, the products are not limited solely to the executive echelon. Intelligence officers and analysts are important secondary consumers of CISC warning intelligence. These intelligence practitioners are key partners in the production of strategic early warning intelligence and are well-placed to identify emerging threats and to detect subtle changes in local threat conditions. Additionally, front-line investigators constitute the third level of warning intelligence consumer. While the appeal and perceived usefulness of these products to the investigator is more limited, these front-line officers are nevertheless vital to the strategic early warning process, as they are often both the first to identify the earliest indications of an emerging threat, and also those primarily responsible with dealing with a threat once it emerges. The goal with this latter audience is less to aid in decision-making than to facilitate situational awareness among the eyes and ears of the intelligence community. It is hoped that by simply scanning the assessment, the officer will internalize the warning so that, when later confronted with new indications, the member will be able to recognize them as such and take whatever action is deemed most appropriate (ideally, sharing this information with the intelligence community).

ii. Principles of SEW reporting—Strategic warning intelligence is intended to alert decision- and policy-makers of an approaching threat so that appropriate action can be taken to avert it or at least mitigate its negative impact. The clarity of the warning judgement in a *Sentinel Assessment* is therefore of paramount importance. Each *Sentinel Assessment* sets out to address a single warning problem, which can be expressed as a specific question with an equally specific answer on the potential for a threat scenario to be realized—"Fence sitting" on threat issues is not a luxury of the warning analyst. The *Sentinel* is therefore designed such that the consumer, after reading the warning notification on the cover page, should know what the analysts believe is most likely to occur with respect to a particular threat issue. This judgement is restated and further qualified at the end of the document to ensure that the warning has been clearly communicated. The remainder of the

Sentinel is intended to provide the context and rationale for this warning judgement, and what this possibly means to the law enforcement decision-maker, in a concise, practical and intuitive format. An upper limit of eight pages (four double-sided pages, including one page for the methodology key and one page for a general explanation of the *Sentinel Assessment,* acknowledgements and contact information) ensures that each *Sentinel* can be read in less than 10 minutes. Colour-coded scales are one means to convey meaning quickly and intuitively while reducing the amount of text needed. Lastly, the use of both print and electronic versions of the *Sentinel* products balances ease of distribution with the need to accommodate a preference among some senior officials for hard copies.

iii. Evaluation and feedback—Measuring results for an early warning system is problematic for a number of reasons. For instance, the accuracy of criminal forecasts can only truly be evaluated if a threat is not prevented (that is, the forecasted threat emerges), in which case the warning function has failed. If, on the other hand, the forecast helps to prevent or limit the emergence of a threat, as it is intended to, then it could later appear as though the warning was a false alarm—a paradox known as the self-negating prophecy. Given these and other challenges, we gauge our success primarily on how our principal client—the Canadian law enforcement community—evaluates the value and quality of our assessments.

To this end, each recipient on the *Sentinel* distribution list is sent a short client satisfaction survey to solicit feedback on the quality and value of the product. For the *WatchList*, the assessed quality/value areas include: writing; clarity of aims; value; relevance of issues covered; and, overall quality. The satisfaction survey for the *Sentinel Assessment* addresses: timeliness; presentation; analysis; information; usefulness; and overall quality. Responses are collected using a scale of 1 to 5 (lowest to highest) for each category, with the option of no response (or "NA"). The surveys also provide for written feedback in the form of comments on how the product could have been improved, and suggestions for future issues. All feedback data from the completed surveys are compiled in a database, where basic statistical procedures are applied to evaluate product performance and identify areas for improvement.

We rely on client surveys as a primary measure of success for the key reason that, regardless of the accuracy of our forecasts, if the community does not regard our assessments as providing added value to its work, then the documents will simply not be read—rendering questions of veracity moot. Nevertheless, accuracy and perceptions of value and quality are intertwined. A mechanism is therefore needed that holds SEW analysts accountable to their analytical judgements and forecasts. The *Sentinel Report Card* is a document used by the SEW analysts and managers to keep track of the forecasts issued so that they can be evaluated over time for their veracity. Whether a situation played out as anticipated or, instead, in an unexpected manner, a comment under the relevant Threat Issue section in the *WatchList* will inform the reader of that fact. This promotes greater transparency and openness in the analytical process by alerting the reader when, how, and why judgements have been modified, appended, or retracted. Figure 19 below shows the basic structure of the *Report Card.*

				Estimated Timeframe (months from date issued)										
Threat Issue	Judgement	Probability	Date	6	12	18	24	30	36	42	48	54	60	Evaluation
Threat heading	Specific forecast	HIGH	Date issued			🟧	🟧	🟧	🟧					Result

Figure 19 – *Sentinel Report Card* template. This performance measure is displayed as a matrix, with *Sentinel Assessments* listed by row, and details of each *Sentinel* displayed in corresponding columns. The result is a single page listing all principal judgements and the degree to which they were sufficiently accurate and precise.

III. CHALLENGES AND LIMITATIONS

Strategic early warning for criminal intelligence faces a number of challenges, some of which are inherent to intelligence work and the warning mission in general, while others are specific to the project in particular. The most fundamental challenge is an epistemological one, and stems from the very nature of the warning mission: the future is inherently unknowable and yet we are trying to speak with some degree of confidence about events that have yet to occur. We make a distinction here between predictions and forecasts. A prediction is the product of a guess—educated or otherwise—about the future; forecasting, on the other hand, involves extrapolating from the data and from observed events to make informed judgements on the future course of particular patterns, trends or phenomena. That there will be another World War before the end of the 21st Century is a prediction; that the eastern expansion of methamphetamine will continue and lead to an increase in property crimes and assaults in the Atlantic region within the next 36 months is a forecast. Predictions are often mere postulations; forecasts are extrapolations and projections from observable facts. The distinction can be subtle, but it is an important one.

While there is often overlap between the two, we are less concerned with predicting the future than with forecasting criminal threats to Canada. While prediction is an intellectual exercise about the future, SEW forecasting aims more specifically at predicting possible and plausible criminal threats to Canada through a series of considered judgements; in other words, SEW analysis endeavours to be an applied social science.[10] Indeed, the methodology outlined herein is neither groundbreaking nor particularly original in its conception—it is simply a novel application of well-established social science principles and methods to real-world problems: organized and serious crime. As such, the epistemological challenge is by no means limited to the field of warning intelligence, nor is it particularly limiting, so long as our task remains focused on rendering forecasts rather than predictions.

A more practical issue arises when we need to render an analytical judgement in the absence of observable indicators. "Fence-sitting" or "wait-and-see" approaches are not options available to the warning analyst; if we are going to write about something in a warning document—whether it is the *WatchList* or the *Sentinel Assessment*—we are going to put forth our best judgement on the potential threat, regardless of whether indicators are visible or not. In some cases, particularly with the *WatchList*, this may mean evaluating a scenario as a medium- or even high-level threat despite having no observable indicators. To some, this may seem to be a glaring contradiction: we develop indicators in order to perceive a threat, and yet, in the absence of indications, we still perceive a threat. While it is indeed difficult to develop a confident assessment of threat level and probability without the assurance of observable indicators, there is no contradiction in formulating a judgement in the absence of evidence. The adage *'absence of evidence is not evidence of absence'* is particularly relevant here; just as the presence of indicators is not necessarily evidence of a threat's emergence, the absence of those indicators is not necessarily proof that no threat exists.

A number of reasons could account for why indicators have not been observed: the issue has not been on the law enforcement radar; we have not identified and exploited the right sources; indications exist but the 'signals' are lost in the 'noise'; or, no indications presently exist because the expected scenario is years away from emerging. Whatever the case, it is important to note that, although warning judgements are *informed* by the observed indicators, they are not *subservient* to them; analytical reasoning must fill the gaps in evidence—no matter how large or numerous—so that a clear judgement can be presented to the intelligence consumer on the potential impact and likelihood of a given threat scenario.

Perhaps the greatest challenge we face, however, and that which presents the most serious limitation of our methodology, stems from the ambiguity of the outcome we are trying to anticipate. Unlike I&W analysis in other domains, where the outcome variables (such as state failure, nuclear missile launch, or global flu pandemic) are clearly defined, the number of possible outcomes in the criminal domain is virtually limitless.[11] While we have attempted to mitigate this problem by restricting our assessments to analyzing a specific threat scenario (that is, clearly outlining the outcome variable in question), the outcome we are trying to forecast is, nevertheless, formulated on a case-by-case basis. This significantly complicates the warning mission for criminal intelligence. Instead of starting with a known potential outcome and then employing a methodology to forecast and anticipate that outcome, we are, in a sense, left wandering in the dark, constantly looking for the ‘unknown unknown’—the potential threat that we have not even contemplated, let alone identified. This invariably makes strategic early warning for criminal intelligence more *ad hoc* in its practice, and its topic selection more analyst-driven as opposed to outcome-driven. This does not negate the value of this work to the intelligence community, but it does limit the degree to which we can identify and warn of all potential strategic threats.

CONCLUSION

Warning is a hypothesis that is informed by reasoning, knowledge, and, critically, by piecing together and analyzing the indications of a potential threat. Strategic warning analysis is a systematized method for developing and issuing sound warnings to those who need them, when they need them. While strategic warning analysis is not a modern innovation, its application within the criminal intelligence community is a recent development. Although relatively new to the law enforcement domain, strategic warning analysis is neither a departure from established analytical practices nor is it divorced from the broader intelligence cycle. It is, rather, a method of analysis that is uniquely focused on the future and specifically tailored to meet the needs of law enforcement decision- and policy-makers. As such, a different approach is required than the one used to produce assessments of the past or present. Articulating this approach has been the principal focus of this paper. The methodology, as it is presented here, is the product of our collective experience over the past two years developing *Sentinel Assessments* and the *WatchList*. It has evolved through in-depth research, testing, community feedback, and, indeed, through much trial and error. It has also been considerably furthered through the involvement of intelligence and warning specialists from a host of domains, particularly the participants of the two SEW Analytical Working Group meetings held in Ottawa, March 2004 and April 2006, and through our collaboration with the Centre for Security and Defence Studies at Carleton University. Such networks and collaborative, interdisciplinary partnerships are the backbone of the Strategic Early Warning System CISC is committed to building on a national level. By presenting a detailed explanation of the SEW concept and method to the broader intelligence community, this paper marks a milestone in the realization of such a system in Canada.

Notes:

[1] Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College, 2002), p. 4.
[2] Grabo, p. 14.
[3] Intelligence typology from http://www.fas.org/irp/doddir/army/miobc/shts3lbi.htm, accessed 2006-08-03.
[4] Carl von Clausewitz, *On War*, translated by Col. J. J. Graham, notes by Col. F. N. Maude (London: K. Paul, Trench, Trubner, 1918), p. 119.
[5] A parallel can be drawn here between our three-stage SEW process and the "scan, monitor, forecast" model employed by the well-established *Los Angeles Terrorism Early Warning* (TEW) *Group*. The TEW Group pioneered the adoption of indications and warning methodology for the law enforcement counter-terrorism domain, and has been successful in developing a network of fusion centres to facilitate the sharing of information and intelligence on potential or actual terrorist threats to the US homeland. We would like to acknowledge the important contribution of the TEW Group's co-founder, Lt. John P. Sullivan, who has been an instrumental collaborator throughout the development of the SEWS project.
[6] John P. Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence," paper presented at the annual conference of the Canadian Association for Security and Intelligence Studies, Montreal, 21 October 2005. Available On-line at www.nfaic.org/OpenLibrary/Police/Counterterrorism%20Intelligence.pdf
[7] Google News Alerts (http://www.google.com/alerts?hl=en), a free service that automatically scans several thousand news sources on the Internet for user-specified keywords and then emails the results to the user, is one useful tool to help the analyst stay current on what is being published in the open English media on *WatchList* topics.
[8] Original matrix from Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999), https://www.cia.gov/csi/books/19104/index.html.
[9] Grabo, p. 14.
[10] We wish to thank our CISBC/YT colleague, Edwin C. Leung, for contributing valuable insight to this section in particular.
[11] We are indebted to our CISO colleague, Daniel Schwartz, for helping us articulate this key limitation.