INTELLIGENCE AND EARLY WARNING

Lieutenant-colonel Adrian-Cristian DAVID, PhD[*]

***Abstract**: Providing strategic warning to policy makers is a key function of governmental intelligence organizations. Today, globally networked challenges have increased so that warning efforts have become considerably bigger. Within the intelligence community it is recognized that many of the current warning problems arise from continued reliance on analytical tools, methodologies and processes that were appropriate to the static and hierarchical nature of the threat during the Cold War.*

***Keywords**: strategic, warning, challenges, threats, tools.*

Introduction

While the nature of security challenges and the study of security itself have undergone some changes since the end of the Cold War and the terrorist attacks against the United States in 2001, the central mission of intelligence structures has remained essentially the same: preventing surprise. A failure of espionage is considered, due to the implications, much more serious than the surprise as such. That most critical information focuses on this aspect is thus easy to see in: the attack on Pearl Harbour, the coordinated Egyptian-Syrian attack on Israel on Yom Kippur, the invasion of Afghanistan by Soviet forces, the end of the Cold War, the attacks of September 11, 2001 and, most recently, the Russian attack on Ukraine. These are just a few of the "surprises" that have been attributed to the failures of the intelligence structures. Most of these incidents resulted in a series of investigations and inquiries whose explicit purpose was to identify the causes of these failures and recommend the necessary corrective actions. The points of view presented in these reports and also in the academic literature dealing with this subject, emphasize that surprises can be prevented by adequate warning. Warning is an informative function that assists politicians both in analyzing various aspects before they become problems, but also in creating contextualized, coherent frames of reference.

Early warning can be considered as the classical strategic role of intelligence. Therefore, it can be said that nothing is more important in the field of intelligence than providing strategic warnings to policy makers. Surprises due to a proper warning error have many causes. The dominant idea resulting from the study of surprise attacks is that the problem does not lie in the lack of information as such, but rather in the incorrect

[*] Ministry of National Defence, email: acdcristi@yahoo.com

understanding of what the available information means, as well as other difficulties and challenges resulting from cognitive and organizational problems. The literature on conflict early warning and response has an excellent track record, completely ignoring the challenges posed by organizational problems. As one official of a national intelligence structure pointed out, not only the terrorist threat, but also *a series of trends of open borders that challenge traditional intelligence systems and law enforcement practices* need to be taken into account. Given the use of a very broad definition of surprise, the list of new transnational challenges includes organized crime, drug trafficking, illicit arms sales, the spread of disease, radicalization and the geopolitical implications of climate change. In other words, intelligence structures are tasked with monitoring threats to their country's national security interests, which are more diverse, interconnected, and dynamic than ever before. We can say, without mistaken, that we are dealing with a new threat environment. Consequently, in this new threat environment, the task of providing warning (in the sense of generating reliable and actionable information about these challenges) has become considerably more difficult, a fact recognized even by the US intelligence community.

From old to new: the new threat environment

The failure to detect North Korea's surprise attack on South Korea in 1950 led to the creation of a worldwide warning system, with the United States creating an advantage by deploying its regional military commands around the world. When the Soviet Union emerged as the main rival of the United States, the intelligence community switched to an indicator-based warning system, based on the premise that the USSR could not launch an attack without some prior efforts to prepare for war and that, if certain key targets were closely followed, indications of the preparation of an attack could have been discovered. The organization and practices of the intelligence community were shaped by particular geopolitics and the technical requirements of the Cold War. Not surprisingly, the change in the international system and the nature of new threats have created some major difficulties for traditional approaches to intelligence gathering. For a better understanding of these difficulties, the old concept of identifying problems and how to approach them should be examined initially, and later, a focus on the nature of the new challenges and the problems associated with them.

Cold War Threat Environment

During the Cold War, the two superpowers combined global political goals with military capabilities. On each side, the security threats were directly related to the military capabilities and were mainly due to the aggressive intentions of the other powerful actors in the international system. This distribution of capabilities, which is unequal and changing, defines the relative power of states, and their careful analysis can help forecast changes in the balance of power at a given time. The early, obvious, transparent and precise parameters of the Cold War threat implied a sense of certainty through planning. Although there were many surprises during the Cold War, the basic task of US intelligence systems was to monitor the strategic capabilities of the USSR. A primary threat meant that other aspects, such as post-colonial insurgency in other regions such as the Middle East, did not shape the process in the way that *Soviet targets* did, even if they were taken into account. The militarized nature of this target meant that there was a concentration of acquisition of *tangible* technical, military, scientific and economic indicators through specialized clandestine collection mechanisms. The identification of the threat level is achieved by examining the capability and potential of an adversary, its intentions and motivation, but also by identifying one's own vulnerabilities. The method of monitoring and surveillance determines a set of indicators - the movement of population and stocks, changes in the maneuvers of ships and planes, the increase of traffic carried out through the means of communication - and a probable graph of the escalation of a conflict. An alarm signal appeared as soon as an indicator crossed a certain threshold. Of course, there was not always agreement on the exact nature of the Soviet threat. However, the debate evolved around the threat, in terms of what could be measured. In addition, there was a belief that it was possible to overcome the threat and ensure security through known measures. The concept of deterring, which refers to trying to create risks that are so great compared to a possible gain that causes opponents to refrain from engaging in a particular policy or action, existed as an option credible to prevent the implementation of the threat. The threat (in form of actor, intent, capability) was generally known and represented by *reliable and credible information.* These characteristics (and how they were perceived) shaped the intelligence community that emerged after the Cold War.

The post Cold War threat environment

The end of the Cold War led not only to the end of a relatively stable bipolar world order, but also to the end *delimitation* threats. The post Cold War components, the security paradigm, are now much more diverse and diffuse. This is especially true regarding the sources of threats: more nations are involved in managing international affairs than before, although often only regionally. Regional problems have proliferated and threaten international peace and security more broadly. Non-state actors have taken advantage of the insecurity of state actors and regional conflicts and in this context, collective security seems to face more dynamic geostrategic conditions, more numerous areas and fields of interest, smaller and more agile adversaries.

The end of the Cold War brought almost nothing else than the transformation of the information environment. The collapse of the international system in turn led to a collapse of previous assumptions and mentalities. Both developments were accelerated by what was called the information revolution, which in turn had an enormous impact on the information community in terms of the threats, but also the opportunities. Closely related to the information revolution, partly caused by it, is the phenomenon of globalization, which was seen as a *process that involves no more and no less than the transformation of the world,* linking daily life to global structures, processes and events. The compression of time and space as a result of globalization has determined an easy movement of the population, but also of weapons, drugs, information and ideas across multiple borders, being partially responsible for the modelling and proliferation of new types of threats. At the same time, the transformation of the information environment is ambiguous and uneven. Globalization has strengthened certain individuals, groups and elites, destroyed hierarchies, but also created new power structures. It can be considered to have both a fragmentation and an integration effect. This ambiguity itself promotes new insecurities and the changes inherent in them move in opposite directions: the vulnerability of terrorist power moves outwards to markets and international organizations, while the ability to cause vulnerability moves inwards, from classes and groups to the individual.

The concept of *uneven transformations* suggests that the present age is marked by persistent contradictory aspects and its order comes from occasional patterns with diametrically opposite results. The spectrum of new threats is dominated by three interdependent characteristics: complexity, uncertainty and a diminished impact on the geographical space. Both the information revolution and globalization accelerate change and therefore fuel the spiral of complexity. With greater complexity, the degree of uncertainty increases further, and thus the identity and goals of potential adversaries, as well as the time frame in which threats are likely to appear, are marked by uncertainty. Additionally, there is uncertainty about the capabilities one must prepare against, and also the type of conflict or situation one is preparing for. A shift in focus from intended adverse actions to more diffuse and unintended threats such as global warming or financial crises only serves to exacerbate these additional difficulties. In fact, risk and uncertainty are the hallmarks of world politics at the beginning of the 21st century.

Warning in the new threat environment

Most of the changes due to the end of the Cold War continue to disturb the intelligence community quite intensely. Many of today's major analytical problems stem from continued reliance on analytical tools, methodologies and processes that were appropriate to the static and hierarchical nature of the Soviet threat during the Cold War. The tendency is to push the extremely complex post-modern world, new and still undefined, into the outdated mentality of the Cold War, with all that it implies, a tendency to reduce the factors of analysis to territorially delimited national states.

Contrary to this general trend, there is a growing part of the intelligence community, which has come to realize that this changing context has important consequences for the methods and methodologies of strategic early warning. However, even though alternative analysis techniques have existed for many years, they have only recently (and still only intermittently) been applied in the intelligence community. Some of the new approaches used within the US intelligence community are reviewed in two separate subsections, consistent with the two distinct stages of warning: monitoring and identification. Traditional Cold War-era signalling systems were geared toward monitoring activities that had been identified as potentially dangerous, such as strategic missile launches.

In the new threat environment, monitoring moves from a surveillance-monitoring exercise to forecasting, understood in context as a probabilistic assessment focused on general trends. Thus, the nature of the new threat environment requires new types of methodologies to capture the nature of new threats (network, transnational, complex).

The second subsection deals with the second stage of warning, which can be described as an identification function and is aimed at assisting decision-makers in identifying dangerous situations that may not necessarily be obvious. The fact that the history of world politics is full of strategic surprises reveals that early identification of the unexpected has always been a major challenge. It can actually be argued that identification has not become more difficult today, despite the new threat environment. On the contrary, some of the alternative approaches in use can help to open previously closed spaces. However, the epistemological questions arising from the new threat environment are largely ignored.

Monitoring

Monitoring in the new threat environment means first of all that new types of methodologies are needed to identify the nature of new threats (network, transnational, complex), some of which take complex environments into account. In general, monitoring now focuses on forecasting certain patterns or activities. Anyway, the success of the forecast is only possible if the problem to be solved has been very well defined and, of course, it assumes that the threat has been recognized in the sense that it is at least partly known. It is not surprising that current monitoring efforts focus mainly on the threat posed by terrorism. Anticipation then requires an awareness and appreciation of the steps and components involved in preparing an attack, but the possibility of chance and surprise must also be taken into account. The literature distinguishes three broad types of methodologies for estimating and forecasting events that have not been clearly identified:

- trends and patterns;
- frequency;
- probability.

What these methodologies have in common is that they place data collected on an ad-hoc basis in a specific context for use within an operation. If the information is missing - in the sense that no trend, pattern or frequency can be distinguished - the collection of data and information, but also the analysis should focus on the risk estimation regarding the probability of attacks against the vulnerabilities. Indeed, one response of the United States federal government to the lack of information has been to move from a threat-based approach to vulnerability estimation and to *play defensive* instead of developing new warning and indication systems. With this approach, the lack of information is replaced by the comprehensive application of defensive measures. There are other (mostly quantitative) methodologies that go beyond these general and well-established tools. At least four methodologies are developed and could improve the monitoring of terrorist activities: predictive geospatial analysis, data mining technologies*, project* management approach and social network analysis.

Geospatial analysis, refers to the attempt to forecast the place and date of future terrorist attacks by accumulating data on the geographic location of previous incidents. For this purpose, the data is entered in a software application that generates signatures of the threat, such as trends in the tactics, techniques and procedures. Using a geographical interface, this system is able then to identify terrorist hot spots.

The second technique involves data mining technologies. Here, large volumes of data on known terrorists can be harnessed and analysed using data mining *tools* in order to search the existing links and patterns in different databases, to identify anomalies and to anticipate which individuals are likely to carry out terrorist attacks. Data mining tools complement information obtained from HUMINT and SIGINT, helping to identify key actors.

The third technique is based on the use of the project management *approach.* A project management model can be used to characterize terrorist operations in terms of tasks, timelines, and lines of responsibility. Understanding this pattern allows the intelligence community to delay or abort an impending operation by conducting "*What if?*" contingency analysis and directing the systematic search for evidence.

The fourth technique is based on the analysis of social networks. It includes, correlates and visualizes biographical, demographic, religious and social data, identifies connections and relationships between individual actors, sympathizers or groups. Such an approach allows us to understand why individuals radicalize and how they are recruited.

These approaches also present certain limitations. The first approach, ***predictive analysis,*** considers only successful attacks and not failed operations or attempts, so understanding phenomenon in an area with a high frequency of them is not necessarily applicable to regions with rarer events. This approach focuses on incidents rather than people, which limits its ability to predict terrorist behaviour.

On the other hand, ***data mining*** does not allow the efficient collection of information about unknown persons and does not solve the problems related to pattern *recognition.*

Project management approach could generate false alarms because identifying terrorists is more difficult and because the approach is based on a limited set of technical indicators rather than complementary technical factors such as the characteristics of the groups and the character of their leaders. To take terrorism as an example, protecting the state and society through preventive measures is hindered by severe limitations due to the possibility that law enforcement institutions may have terrorist followers, infiltrated among the employees. Threats or dangerous people are usually identified by studying obviously illegal actions or by antecedents.

Finally, ***the analysis of social networks,*** although important, does not complete the overall picture. However, with a careful analysis of the pros and cons and by carefully combining several methods, it may be possible to obtain attack indicators with some predictive potential.

Other types of indicator-based systems are developed in the field of political risk analysis, generally for more complex and diffuse threats. The purpose of these approaches is to build risk databases that attempt to correlate and/or identify specific trigger points with specific risk events. The databases must contain sufficient data to allow the development of indicator models that can identify sequences of events or triggering mechanisms that are precursors to regime instability, conflict, humanitarian crises or any series of other serious events. Such models can lead to reasonable forecasts when data are available and the belief that existing, well-understood and well-defined patterns of behaviour will continue into the future, despite the fact that many aspects of specific challenges may still be undiscovered. In other words, for the monitoring of activities to make sense, there must be the idea that the threat is analytically malleable and that the cause-effect relationships are identifiable. However, there is clearly ***an inherent danger*** in this hypothesis: such certainty about the possibility of knowing could lead to wrong actions, based on full trust in these systems. If there is doubt that the relationships described in the model will continue or if the forecasts on the independent variables are uncertain, various tools are needed.

Identification

Identification is a different field. The concept of strategic early warning is based on the assumption that discontinuities do not appear without warning. Warning signals have been described as *weak signals* or change factors, which are hard to perceive now, but which will constitute a strong trend in the future or which may have significant consequences.

Management *unknowns* makes it necessary to collect *weak signals* and identify events or developments that could signal dynamics and alternative paths. As previously mentioned, the very broad definition of surprise agreed upon by the US intelligence community, which includes anything that can impact it, its allies, or its interests anywhere in the world, makes it very clear why uncovering such signals is a difficult task. The concept of identification does not refer to the recognition of the pattern or known patterns, but rather to the ***identification of new patterns***. At a seminar on the psychology of information, Heuer[1] talks about their inherent problems, emphasizing that: "we tend to perceive what we expect to observe, to perceive". The author goes further and states that "expectancy patterns become so deeply ingrained that they continue to influence perceptions, even when people are warned about it and try to take into account the existence of data that do not fit their prejudices".

The puzzle of discovery and innovation is fundamental in this context: how will we notice a pattern we have never seen before? There is always an ad-hoc quality regarding the recognition of new phenomenon and the ontological validity of perceived novelties remains unclear. Because patterns must be *recognized* by the observer, any observed pattern or structure may be ***the subject of a research direction,*** at the same time and for the same reasons, other patterns may go unnoticed. The cognitive limitations of decision-making analyses lead individuals to use simplified strategies to ease the task of mentally processing information and dealing with complexity and ambiguity. As Snowden[2] explains, when one examines data, only a small percentage of the visual beam is precisely focused, with the human brain filling in the gaps. This process of pattern recognition can cause patterns to appear or weak signals to be lost – *we don't see them because we don't expect them to be seen.* In a complex system, where the number of possible connections can be very large, the ability to see is overwhelmed with possibilities. Such behaviour leads to predictable faulty judgments known as cognitive biases.

[1] Heuer, Richards J., Jr., 1999. *Psychology of Intelligence Analysis.* Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.

[2] Snowden, Dave, 2002. 'Complex Acts of Knowing: Paradox and Descriptive Self Awareness', *Journal of Knowledge Management* 6(2): 100–111.

In the context of discovery, the type of bias of great importance is called model bias, which prompts the search for evidence that confirms rather than rejects a hypothesis and fills in missing data with data from previous experiences[3]. Another problem in this context is the challenge of ethnocentrism, i.e., *the tendency to judge the traditions/ objections of other societies according to the standards of one's own culture*. In the field of identification, ethnocentrism influences how signs are read and will lead to several patterns of prejudice. How can these problems be overcomed? Over the years, public and private sector organizations have developed tools for what is called *alternative analysis,* "techniques that seek to help analysts and policymakers expand their thinking by expanding the range of proposed outcomes or challenging fundamental assumptions"[4].

"There are many methods that can be used as future methods, it is enough to indicate the most prominent of them: developing scenarios, Delphi exercises and scanning the horizon for managing the future, brainstorming etc."[5]. Snowden describes, also by a set of narrative methods, which provide a rich context that allows the emergence of models/examples of experience rather than opinions or beliefs. An approach that is often stated to maximize weak signal detection in a complex system is called horizon scanning. The main advantage of these techniques is that they can stimulate strategic thinking and communication, improve internal flexibility to respond to environmental uncertainties, and provide a forecast basis for possible system failures. However, they also do not return *certainty.*

Alternative analyses are designed to overcome biases: their use does not necessarily mean the possibility of estimating the future. If they are conceived as a set of tools, rather than an ongoing organizing process aimed at promoting sustained, sustained attention, they are unlikely to be accepted within the community. Moreover, there is always the danger that these approaches will be disapproved of for directing attention to outcomes that

[3] Johnston, Rob, 2005. *Analytic Culture in the US Intelligence Community: An Ethnographic Study.* Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency;

[4] Fishbein, Warren & Gregory Treverton, 2004. 'Making Sense of Transnational Threats', *The Sherman Kent Center for Intelligence Analysis Occasional Papers* 3(1);
George, Roger, 2004. 'Fixing the Problem of Analytical Mind-Sets: Alternative Analysis', *International Journal of Intelligence and Counter-Intelligence* 17(3): 385–405;

[5] George, Roger, 2004. 'Fixing the Problem of Analytical Mind-Sets: Alternative Analysis', *International Journal of Intelligence and Counter-Intelligence* 17(3): 385–405.

may be almost improbable by definition, diverting political attention and resources from far more likely threats.

Conclusions

A requirement critical to effective warning in the 21st century threat environment is sensitivity to complexity. Analists will need to use current hypotheses and insights, engage in pattern discovery, forge closer ties with policy makers to enhance their sensitivity to issues, and engage in systematic probing strategies to gain knowledge and understanding adaptive responses. In addition, the assessment and monitoring of multiple surveillance points in turbulent spaces will be essential, as will the use of open sources of information and multiple sets of indicators. It is important to recognize the dynamism and evolution of complex systems.

Therefore, "constant processing and adaptation are necessary to ensure that the warning itself becomes a complex adaptive system"[6]. Obviously, this means that horizontal knowledge networks must be adapted, even at the cost of vertical integration. The traditional model of the individual annalist at the center of the information process is moving away or disappearing.

All of these alternative approaches described above work best when a mixed group of people with diverse backgrounds is created to work together. But before trying to revolutionize the entire system, the intelligence community should try to separate traditional threats from less understood problems[7].

It can be argued that the most important conclusion that can be drawn is that the solution would be found in a political discourse about uncertainty. The tension between the need to know (and the desire to know, to the same extent) and the end of certainty is linked to a functional and, in particular, political necessity to maintain the myths about control and administration, because they represent the most or subsequent requirements. The myth of perfect administration must be overcome and an explicit

[6] Williams, Phil, 2006. '21st Century Challenges to Warning: The Rise of Non-StateNetworked Threats', in Center for Security Studies, ed., *Workshop Report, Global Futures Forum: Emerging Threats in the 21st Century, Seminar 1: The Changing Threat Environment and Its Implications for Strategic Warning.* Zurich: Center for Security Studies.

[7] Rolington, Alfred *"Objective Intelligence or Plausible Denial: An Open-Source Review of Intelligence Method and Process Since 9/11", Intelligence & National Security* 21(5): 738–759.

discourse on the possibility of failure and especially on its potential causes and subsequent steps to minimize the damage produced is necessary. Governments and government agencies should not act as if all risks are under control and under no circumstances challenge contrary assumptions, even from the media, about these risks. This seems to be the only way out of the vicious circle that has created uncertainty for organizations dedicated to gathering actionable information. Also, this would counter at least part of the danger that uncertainty is used from a political point of view, to legitimize other types of actions.

BIBLIOGRAPHY

BENDOLY E., WEZEL W., BACHRACH D., *The Handbook of Behavioral Operations Management. Social and Psychological Dynamics in Production and Service Settings,* O ford University Press, Oxford, USA, 2015;

BETTS, R. K., 1982. *Surprise Attack: Lessons for Defense Planning.* Washington, DC: Brookings Institution;

CHIFU I., NANTOI O., *War informative. Typification MODEL aggression*, Publishing House Institute of Political Sciences and International Relations *Ion IC Brătianu*, Bucharest 2016;

COKER C., 2002. *Globalization and Insecurity in the Twenty-First Century: NATO and the Management of Risk,* Adelphi Paper 345. London: International Institute of Security Studies;

COMBS D., 2008. *Inside the Soviet Alternate Universe: The Cold War's End and the Soviet Union's Fall Reappraised.* University Park, PA: Penn State University Press;

COOPER J. R., 2005. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis.* Washington, DC, Center for the Study of Intelligence, Central Intelligence Agency.

ELIAS C., *SCIENCE OF THE ROPES. Decline of Scientific Culture in the Era of Fake News,* Springer Publishing, Cham, Switzerland 2019;

ULRICH B., 1999. *World Risk Society.* Cambridge: Polity;