"Emerging Threats in the 21st Century" Strategic Foresight and Warning Seminar Series

Final Report

Zurich, December 2007

CSS
An ETH Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contact:
Center for Security Studies
Seilergraben 45-49
ETH Zürich SEI
CH-8092 Zurich
Switzerland
Tel.: +41-44-632-40-25
css@sipo.gess.ethz.ch

Global Futures Forum
Emerging Threats in the 21st Century

Final Report
December 2007

Organized by:

Center for Security Studies, ETH Zurich
Global Futures Partnership
Co-sponsored by the US National Intelligence Council

Table of Contents

Preface

Over the course of the 2006-2007 academic year, the Center for Security Studies at ETH Zurich and the Global Futures Forum – a multinational, multidisciplinary, and cross-sector group formed in November 2005 at an international conference hosted by the Global Futures Partnership of the US Central Intelligence Agency – joined efforts to conceive of new ways of thinking about strategic warning in the changing global security environment. Together, the Center for Security Studies and the Global Futures Partnership planned and organized a series of three seminars on Strategic Foresight and Warning, bringing together the ideas, intellects and expertise necessary to increase our understanding of the challenges faced by analysts the world over. The seminar series was designed to facilitate the formation of an active, vibrant, and self-sustaining community of warning experts. Over the course of the three seminars, participants also took part in a series of breakout group sessions to stimulate debate on key issues in strategic warning. The results were elucidating and thought-provoking.

Creating and coordinating an effective warning capacity – one that is capable of identifying and responding to potential upheavals – is essential to national and international security. Indeed, providing strategic warning to policymakers about potential threats and dangers is a key function of governmental intelligence organizations, one by which their performance is most stringently judged. However, the context for warning is rapidly changing, particularly as globally networked threats overshadow their historical state-centric counterparts. Many of these threats can be defined as transnational, clandestine, networked, adaptive and connected (participates in a global network and the global economy). Their scope, scale and complexity have placed unprecedented strain on the security and stability of the international system.

The challenges inherent in warning about such changed threats stem from an asymmetry of vulnerability, a wide "signal-to-noise" ratio, and lack of stable indicators that can be used to monitor trends. The strategic picture is constantly changing and there are always the "unknown-unknowns" that need to be identified and addressed. The very openness of the international system to rapid and potentially destabilizing changes makes it still more vulnerable to upheaval.

While warning has typically focused on shorter term risks, it is increasingly apparent that analysts should also work to discern more distant theats along with future opportunities. This would allow policymakers to take early corrective action to shape the strategic environment rather than only be in a position to react to situations where options may already be very limited. Processes and vehicles for warning must also be updated to take into account the fact that the client base for warning has expanded well beyond senior political and military leaders to include a wide range of decisionmakers at the national, regional and local levels. However, for all its attractions and promise, the business of strategic warning is notoriously complex.

The most common challenges encountered in warning can be clustered into three broad categories: bureaucratic (connecting silos while preserving operational security); cognitive tapping into the knowledge of the private sector and of diverse intellectual disciplines, challenging mindsets, and enhancing weak signal detection); and technical (sharing open and sensitive data, developing and implementing the right tools to enable pattern-matching, automated indexing etc.).

These challenges were explored in considerable detail over the course of the three seminars. Below we summarize the major foci of discussion: the need for organizational change, improved intelligence analysis, superior warning tools, and improved relations with policymakers. Key points and recommendations to the intelligence and strategic warning community have been provided in the Executive Summary of this report.

Dr Warren Fishbein
Deputy Director
Global Futures Partnership

Professor Dr Andreas Wenger
Director
Center for Security Studies
ETH Zurich

Executive Summary

The Organization of Intelligence

Of crucial importance in the strategic warning debate is the need to create new organizational structures, workflows, processes and cultures. Participants were of the opinion that most intelligence organizations focused on immediate results rather than long-term gains. Organizational structures are often reinvented to solve yesterday's problem rather than tomorrow's priorities.

The "high-reliability organization" was held up as one ideal that the intelligence/warning community should emulate. These organizations are flexible, resilient, and quick to adapt to a rapidly changing security environment. They are driven by a commitment to public service and operational excellence and are capable of conducting relatively error-free operations over a sustained period of time. Moreover, they are capable of fostering effective interoperability within and between one or more organizational units. How does one establish such an organization? What are its defining features?

High reliability organizations have first class communication and information management policies in place so as to make best use of the intelligence they collect, analyze and disseminate. In addition, they champion the idea of organizational learning and knowledge sharing. For such knowledge-sharing efforts to be successful, the upper echelons must give their full support to intra- and inter-organizational collaboration. Such activities can be incentivized through a rewards system. Where appropriate, these organizations have also adopted the use of collaborative tools as a means of breaking down organizational walls and improving the quality of analysis on this and other security issues.

Effective warning also requires that these organizations demonstrate a high degree of trust, thus opening perceptual blockages to weak signals, enhancing communication and horizontal integration, and moving decision making to lower levels of the organizational hierarchy as necessary. Most security crises are not the result of a "single discipline problem". As such, high reliability organizations have to cultivate a variety of responses. They must be open to interdisciplinary thinking and closer collaboration with third parties from academia, the private sector and civil society. Only through a rigorous process of change can the intelligence community hope to institute a new professional ethic that will alleviate the threats it currently faces.

On the issue of organizations, key recommendations included:

- Conduct a thorough human capital assessment that would offer human resources personnel to identify and employ recruits with the relevant skills.
- Develop a common lexicon of security-related terminology and a catalog of best practices to better understand and address 21st century security threats.
- Cultivate a more holistic approach to intelligence work on the physical, information and cognitive domains.
- Mimic adversaries in terms of thinking, analysis and organization and by learning to adapt, to morph and to engage in bottom-up behavior.
- Give more room within organizational structures for skeptics and "maverick" thinkers.
- Work to bring down organizational information silos and to remove the walls between data analysis and collection, and between intelligence analysis and intelligence operations.
- Cultivate lateral cooperation with other intelligence organizations, even if this can only be done via "unofficial" channels. Relations between different intelligence or security actors should be built and sustained before the need for information sharing arises.

Towards a New Analysis Paradigm

The challenge of effective warning, it was argued, stems not from a problem of information collection but rather from one of analysis. Thus, all three seminars examined intelligence analysis in light of changing trends in the global arena as well as previous "intelligence failures". How should the intelligence community respond to these problems and thus create a new paradigm for analysis?

To begin, there is the issue of personnel recruitment. The intelligence community has to overhaul its recruitment policies in order to identify and train those individuals that are better equipped to deal with the cognitive challenges of information processing and analysis. Recruiters should forego those individuals who seek "cognitive closure", or rather the desire for a confident judgment on an issue as compared to ongoing confusion and ambiguity. These individuals also have a tendency to view things from their own organizational or empirical perspective, thus limiting their ability to appreciate novel approaches to today's security threats.

There are no one-size-fits-all solutions to the problem…

Intelligence analysts and warning practitioners have to be more comfortable with a relatively high degree of confusion and ambiguity. They must be amenable to changing their mental models in order to address a growing variety of problems. Intelligence is increasingly seen as work in progress, one that's never finished. Analysts must learn to adapt their approaches to collecting, synthesizing and interpreting the information they are given. Indeed, some have signaled the need for more synthesists in the intelligence community. These individuals would complement the regular analytical work by providing or emphasizing probabilities rather than predictions, uncertainty rather certainty, better questions rather than better answers, and hypotheses-based rather than evidence-based analysis.

Analysts must accept there are no one-size-fits-all solutions to the problem of intelligence analysis or warning (nor, indeed, is a single technical tool sufficient either). Conducting an analysis on a single premise is unwise, regardless of whether it is based on empirical evidence or expertise. No matter how thorough a horizon scanning exercise might be, analysts must still plan for and anticipate "wild cards". A portfolio of skills has to be brought to the job or given to every analyst through further training.

In terms of alternative analysis approaches – analysis specifically designed to challenge analyst and policymaker assumptions – participants spoke of the importance of structured analogies, role-playing, story telling, and cognitive mapping. They also referenced the use of prediction markets as instruments that can be applied to the business of strategic warning.

Further, analysts must develop and use fresh assumptions and engage in pattern discovery in addition to the more traditional task of pattern recognition. They must forge closer links with policymakers to enhance their sensitivity to the issues being explored, and then collaboratively engage in systematic probing strategies to elicit knowledge and understanding of the adaptive responses of networked threats. For long-term planning to be more relevant, it has to avoid Western biases – not everything is the product of Euro-Atlantic activity – and take into account long-term historic trends. Thus, a closer reading of world history and improved understanding of global opinions are both essential.

The traditional model of the individual analyst at the center of the intelligence process has started to recede. Expertise will matter more in terms of how it describes the complete expertise of a collaborative group. Expertise in collaboration will become more important. The intelligence community was further encouraged to mimic its adversaries in terms of thinking, analysis and organization by learning to adapt, morph and engage in bottom-up behavior. Essentially it must learn to better manage the complexity it creates for itself.

Inevitably, no single analytical or methodological technique is sufficient to address or understand a given problem. Instead, different approaches should be attempted or combined as necessary to maximize the accuracy of results.

On the topic of analysis, key recommendations from the seminars included:

- Enhance the tradecraft of intelligence analysis to include methodologies and approaches for dealing systematically with incomplete information, complexity, uncertainty and futures analysis.
- Bring in outsiders (e.g. from the private sector) to enable improved understanding and "out of the box" scenarios and to supplement internal intelligence analysis.
- Foster interdisciplinary research and thinking on today's most pressing security challenges.
- Broaden the aperture of intelligence analysis, especially in terms of history, time and scope.
- Introduce analysis techniques early on in the process of data collection so as to help overcome the problem of information overload.
- Learn to adapt different approaches to collecting, synthesizing and interpreting intelligence information.

The Strategic Warning System

Participants devoted a considerable amount of time defining the optimal warning system. There was general consensus that warning system should be flexible, extendible and transboundary.

Some participants recommended that the establishment of a transboundary warning system should be preceded by a study of transboundary networks that share information (such as the international weather and media networks) to anticipate challenges and incorporate useful innovations.

Once in place, this system should monitor more than just existing or emergent security concerns. It should also consider currency markets, trade flows, subtle changes in standards of living, and political activities that may be precursors of something more significant.

An effective strategic warning system should also allow for a range of analytical methodologies including geo-spatial predictive analysis, data and text mining, data visualization and social network analysis which identifies the connections and relationships between individual actors, enablers, issues, entities or groups. By accommodating different branches of knowledge and expertise, multilinguality, extensive cultural understanding, and access to rich data sources and different opinions, the system should be better able to track a broader range of issues than those of concern to traditional security and intelligence organizations.

From the standpoint of the participants, key recommendations for the warning system include:

- Maintain a long-term perspective when implementing a warning system.
- Tailor strategic warning to meet strategic goals defined by customers.
- Understand that warning systems have to be adapted to the "administrative sociology" of the organization or country in question.
- Broaden the focus of warning systems beyond simply preventing surprise to warning about different trends, social movements, and opportunities as well.
- Learn to work with visualization tools that can aid the understanding of complexity or the richness of social networks.
- Establish a "history of warning and foresight" as a way of tracking the evolution of the discipline.
- Establish a strategic warning system that monitors activities in other sectors (e.g. the financial markets) as well as traditional security or law enforcement vectors.

Relating to Policymakers

Finally, participants affirmed the need to strengthen relations with the policy community through a series of small steps, the first of which is improved communication. This is a key factor in successful warning and longer term strategic foresight. No investment of time or effort here is too small.

The traditional boundaries of the intelligence/policy nexus have to be reconsidered and redefined as part of an ongoing, iterative process. Policymakers need to be given a sense of ownership in whatever issue the intelligence community has been asked to address. By doing so, the intelligence community would be better placed to convince decision makers to allocate greater resources to dealing with those issues that pose the greatest threat rather than those which are popular or media friendly.

The analysts themselves must present and clarify the policy choices available (together with their implications) in a manner that is clear and unambiguous. Effective communication should thus help policymakers to identify the risks, delineate the impact if something should happen, connect the future to their interests and prepare accordingly. As one speaker put it, effective warning is an "invitation to the recipient to act".

The traditional boundaries of the intelligence/policy nexus have to be reconsidered and redefined…

Improved communication should also enable analysts to better understand the policymaking process and their clients' objectives. Policymakers will not necessarily shy away from difficult issues but intelligence providers must meet policymakers' needs for material that is persuasive not only to themselves but also to their peers and superiors. Just as important as working with policymakers is working with the public. A systematic and patient process of generating public awareness should enable the intelligence and warning community to cultivate enlightened communication about risk and threat perceptions. Further, good risk analysis requires salesmanship to convince, mobilize and win support for the necessary action.

On relating to policymakers, participants related the following key recommendations:

- Invest more effort in understanding the needs, expectations and objectives of customers (e.g. policymakers).
- Convince decision makers to allocate and time and resources to where the real risks are and not only to "popular" issues.
- Present policymakers with a variety of scenarios based on different vectors of action.
- Where necessary, develop and recommend low-cost hedging strategies against possible threats so as to keep policymakers better informed as indicators develop and change.
- Engage the general public by acknowledging societal vulnerabilities and asking them to play a more active part in ensuring public safety.

Listed below are synopses of the thoughts and recommendations given to the intelligence and strategic warning community by speakers, commentators and participants at each of the seminars. The work that took place during the breakout sessions is also integrated into the synopses.

Seminar I: The Changing Threat Environment and its Implications for Strategic Warning

Zurich, 9-11 November 2006

The key objective of the three seminars was to explore new ways of thinking about strategic foresight in a significantly altered and rapidly changing international environment. To this end, The GFF convened over 70 intelligence experts and speakers from fields as diverse as complexity theory, networks, cognitive biases, and forecasting, among other salient areas of enquiry.

During this seminar, three explanatory factors for the new international environment were explored: increasing complexity, decreasing predictability, and the changing importance of geographical spaces. These factors were elaborated upon to include the following:

- The range of threats has become highly complex due in large part to greater complexity in the post-Cold War era. There is a growing number of independent international and transnational actors playing power games on multiple levels revolving around national, regional, and global dynamics.
- Current threats are less predictable than traditional state-centric threats and come from more diverse sources. The level of uncertainty in the world has increased significantly since the end of the Cold War. Computer hackers and criminals, disaffected domestic groups, natural and man-made viral borne illnesses, and radical terrorists, including those motivated by Muslim fundamentalism, are all representative of these new threats.
- International affairs have become more decentralized and regionalized since the end of the Cold War. Due to globalization more nations and non-state actors than ever before are active on the international level, albeit often only on a regional basis. Regional issues have proliferated and often appear to threaten wider international peace and security. Terrorist groups and other non-state actors have taken advantage of regional conflicts and insecurities.

This changing context reveals substantial effects for strategic warning. In particular, warning is being transformed from an exercise in surveillance, i.e. monitoring identified and known indicators (such as the mobilization of a military), to one of "reconnaissance," or searching for signals of potential, perhaps unknown threats that could potentially emerge anywhere or at any time. Thus, the key problem is not necessarily information collection or its lack, but rather analytical difficulties and challenges arising from cognitive and organizational issues. During this first seminar, participants identified key challenges to effective warning on three, at times overlapping, levels: the individual, organization and customer.

Individual	concerns cognitive and analytical issues and “the analyst”
Organizational	concerns intelligence organizations
Customer	concerns the interaction between analysts and policy-makers

The Individual Level

On the first level, features of human cognition impede the delivery of better analysis. Cultural biases, or the effects of small-group processes, need re-examination. Potential solutions to such problems could include recruiting and training analysts who are better equipped to deal with the cognitive challenges of information processing and analysis in the changing environment. During the first seminar, participants learned that specific personality types are better suited to the business of strategic warning and intelligence analysis.

Thus, a thorough "human capital assessment" would offer prospective employers an opportunity to identify recruits with the relevant skills, whether innate or learned. Other solutions that were discussed include the institutionalization of the role of "devil's advocate", enhanced mechanisms of information flow, improved formal education on the part of the intelligence analyst, and the implementation of ethical standards for analysts. It was noted that a type of synthesis could complement the regular analytical process by providing or emphasizing probabilities rather than predictions, uncertainty rather than certainty, better questions rather than better answers, and hypothesis-based rather than evidence-based analysis. Concepts drawn from epidemiological efforts to monitor and warn of outbreaks of disease might similarly be used to support warning efforts focused on other forms of contagion, such as the spread of violent forms of political radicalization. To identify tools and techniques for alternative analysis, the experiences of the private sector as well as the public sector should be taken into account.

…synthesis could complement the regular analytical process by providing or emphasizing probabilities rather than predictions, uncertainty rather than certainty, better questions rather than better answers, and hypothesis-based rather than evidence-based analysis.

On the individual level analysts must acquire and employ the appropriate methodologies. The managerial level has to constantly review and refine these methods by adapting them to a rapidly changed threat environment.

The Organizational Level

On the organizational level, the problem of "group-think" can lead to intelligence failures. In addition, new information that is inconsistent with existing preconceptions is often simply rejected. There is great need for cultural change within the intelligence community, in particular with regard to accommodating different cognitive approaches, organizational "mavericks", and skeptics who aren't afraid to think differently and communicate bad news.

…the rigidity of fixed assumptions is another inhibitor of strategic warning

On the matter of organizations, it was noted that the success of the US warning system during the Cold War has made it difficult to change today. The principle of US intelligence – that every analyst is a warning analyst – confers responsibility on everybody. Ultimately, however, responsibility to act rests on no one. Creating a "culture of vigilance" with permanent focal points that enable coordination, communication, outreach and quality control may go some way to mitigating this problem. Establishing more creative and experimental structures, emphasizing the need for organizational learning, and improving intolerance for mistakes would improve people's willingness to take responsibility and act.

The rigidity of fixed assumptions is another inhibitor of warning, especially in a rapidly changing security environment. To overcome this problem, the intelligence community has to create organizational cultures that challenge institutional processes and mindsets. One way of doing this would be to bring in external expertise as a way of challenging assumptions. Another approach might involve the public sharing of intelligence analysis in order to open it to public scrutiny. On the institutional level it is essential that a permanent dialogue between the warning community and policymakers be established.

Finally, on the issue of "sense-making" it is important that a warning system allow for the cross-referencing of contacts, self-critique and self-review, and intuitive thinking. It should also make greater use of the wisdom of crowds and prediction markets.

Intelligence communities will have to mimic adversaries (in terms of thinking, analysis, and organization) by learning to adapt, morph, and engage in bottom-up activities in order to adapt to the global borderless intellectual space. Rather than trying to destroy old organizations or create new ones in their stead, one fruitful approach might be to operate at the "edge" of organizations. It would be ideal if those "edges" could come together in collaborative workspaces, probably virtual ones. The private sector could be one

place to find lessons on implementing successful cultural change, while NGOs could offer useful advice on cultivating radical thinking. In addition, the new threat profile requires reaching out to other like-minded states and to multinational groups of experts.

The Customer Level

There is immense need to work more closely with customers (e.g., policymakers). However, due to the shifting environment, the very nature of the "intelligence consumer" appears to be evolving. Federal policymakers, but also state and local leaders, as well as the media and the public, are all intelligence consumers. As policy and policymakers become more diffuse, it becomes harder for the intelligence community to connect with policy. As there is no standard definition and no "typical" intelligence customer, an improved understanding of each other's needs is necessary.

Understanding and serving the needs of policymakers is perhaps the greatest challenge to the strategic warning community. Products have to be tailored to the client's needs, which are subject to considerable change. Indeed, a well-tailored process – one that remains neutral in so far as possible - may often be more important than the product itself.

However, questions regarding the proactive approach remain. For example, should intelligence analysts "market" intelligence analysis to policymakers? Should customers be more closely involved in the business of strategic warning mapping and reporting? To answer these questions, it may be worth looking at other models of collaboration as well as "best practices" in other countries or in other sectors.

…every analyst is a warning analyst

Two breakout group sessions on the topic of warning systems were held. During the first (10 November 2006), participants were asked to elaborate on those elements that constitute an effective warning system. During the second session (11 November 2007), participants were asked to consider the challenges to implementing an effective warning system with regard to existing organizational structures, sense making, relations with policymakers, and existing intelligence assumptions.

There was general consensus that the objective of a warning system is to enable informed action and provide enough lead time for mitigating risks. Thus, it should allow for improved communication between analysts and decision makers and enable all parties to better understand each other's needs. It should also enable horizontal and vertical information-sharing as well as the opportunity to build fluid communities of interest that can be integrated into the various institutional structures.

Participants stressed the importance of "warning education" to support the warning process – to enable customers to better understand the work involved as well as clarify exactly what they wanted to be warned about – and the need to engineer the intelligence community so that that it is better suited to running a warning system.

Seminar II: Sense-Making and Warning – How to Understand and Anticipate Emerging Threats

Zurich, 19-21 January 2007

The second of the three seminars built upon the theoretical foundations presented in the first seminar and focused on methodological approaches for establishing strategic warning systems. It concentrated on concrete methods, instruments, and tools. Presentations were delivered on traditional warning methodologies, cognitive mapping, horizon scanning, quantitative models, and other foci.

Traditional Warning Methodologies

Indicator-based approaches to warning include monitoring and surveillance methods for tackling traditional threats. Such methods seek to define a set of indicators and a possible timeline, for example the escalation of a conflict. Once a (large) set of indicators has been established, a warning signal emerges as soon as an indicator reaches a certain stage. The analyst does not analyze the data in the strict sense of the word, but feeds significant amounts of collected information into the system, watching and waiting for indicator movement. Although these indicator-based approaches are generally artificial to some extent, they possess important strengths: first, they allow for a certain degree of objectivity in assessing situations; second, they require analysts to anticipate potential future developments on the basis of scenarios.

The challenges inherent in warning for contemporary and emerging threats stem from the asymmetry of vulnerability, the low ratio of "signal-to-noise", and the lack of stable indicators that can be used to monitor trends.

The main weakness of this method, however, is that analysts must know in advance the threat that the system is designed to warn of. This approach may work fairly well for clearly definable traditional threats, but it is not suited for diffuse, unspecified risks and is particularly inadequate for the detection of emerging risks that are not yet on the watch-list. The challenges inherent in warning for contemporary and emerging threats stem from the asymmetry of vulnerability, the low ratio of "signal-to-noise", and the lack of stable indicators that can be used to monitor trends. The strategic picture is constantly changing, and there are always "unknown unknowns" that need to be identified.

Traditional warning methodologies can work well once the shape of the threat has become clearer. For example, data-mining technologies can be used to forecast terrorism using large volumes of data on known and potential terrorists to identify links, patterns, and anomalies, and to predict which individuals are likely to carry out terrorist attacks.

Weak Signals, Sense-Making, and Warning

The concept of strategic warning is based on the assumption that discontinuities do not emerge without warning. These warning signs have been described as "weak signals", or factors for change that are hardly perceptible at present, but may (or will) constitute a strong trend in the future or can have dramatic consequences. Typically, five stages can be distinguished during which weak signals develop into strong signals:

1. The weak signal emerges
2. The source of threat becomes known
3. The shape of threat becomes concrete
4. The response strategies are understood
5. The outcome of response can be predicted.

Clearly, these various stages require different approaches. Is it possible to amplify weak signals without increasing the overall level of noise?

The management of "unknown unknowns", on the other hand, makes it necessary to gather "weak signals" and to identify certain events or developments that could set off alternative dynamics and paths. Therefore, approaches are required that aim to maximize weak signal detection in a complex system, such as horizon scanning. Using the techniques of content analysis, scanning itself relies primarily on examining various media sources, private sector "gray literature" such as working papers and conference proceedings, and other open sources such as websites.

Pattern Matching and Story Telling

The cognitive sciences have demonstrated that human intelligence is based on pattern recognition. People appear to think in patterns and not in streams of logical thought, as was once held. Therefore, weak signals could be detected more easily by taking advantage of the brain's pattern-matching capabilities.

The study of storytelling has become a feature of many disciplines. Previously overlooked, storytelling and the use of narratives are omnipresent. Additionally, storytelling appears to have a profound impact on listeners' abilities to comprehend complex problems. By listening to stories or anecdotes of problems that have occurred in the past, we have a better chance of picking up weak signs of future problems at an early stage, when they are still masked by massive amounts of noise. Taking this into account, Dave Snowden's famous Cynefin framework can enhance the intelligibility of data. The Cynefin model delineates four "spaces": known, knowable, complex, and chaotic. Each of these has a different dynamic, and involves not just a different analytical method, but a different diagnostic method, a different intervention approach, and a different set of supporting tools and technologies. The framework also demonstrates the interaction of structures, processes and uncertain conditions, and can help make sense of the complexities made visible by the relaxation of basic assumptions (e.g., order, rational choice and intent). Pattern experience gives rise to stories (the principle mechanism for knowledge) and story-telling (a primary mechanism for knowledge sharing).

Without a doubt, no single analytical technique can be rated as the most accurate approach to the study of all types of problems. Analysts must apply the methods that are best suited to a given problem and consider combining approaches in order to maximize the accuracy of results. Specifically, analysts should be taught in what situations to rely on heuristic thinking or "gut feeling" and when to use concrete methods, instruments, or tools.

…storytelling appears to have a profound impact on listeners' abilities to comprehend complex problems.

Strategic Warning Systems

When applying these insights to the requirements of a transboundary warning system, the main objectives are to understand the conditions for the emergence of new risks and to identify possible trigger events that could have cascading effects.

Analysts would have to come prepared with expertise, strong language skills, extensive cultural understanding, and access to rich data sources that can provide alternative analyses and varied opinions. In addition, such a system would have to draw on a truly diversified network of contacts that are well-placed, willing, and motivated, and who are able to monitor and report on critical information as well as receive and process such information. Possible obstacles to such undertakings might include the lack of participation of potential future users in the implementation phase, no joint understanding of the nature of "weak signals", differences in system requirements that may be concealed by various interested parties, excessive reliance on ostensible "hard data", a deficiency of interaction among users and, finally, weak integration with the strategic functions of an organization.

Furthermore, in order to become highly reliable organizations that conduct relatively error-free operations over a long period of time, intelligence services must undertake a concerted effort to address the challenges posed by the intelligence community's very structure. They must demolish the walls between data analysis and collection, and between intelligence and operations. They must also demolish that walls that exist within and, where necessary, between intelligence organizations themselves if they are to perform more effectively.

Participants also revisited the task of defining the requirements for a transboundary warning system in light of the following threat scenarios: an Avian Flu pandemic; a revival of conflict between India and Pakistan; sustained high oil prices; the rise of the Shia in the Middle East; and the transformation of terrorism.

To be successful, a warning system should define and share its objectives upfront. Further, it should remove politics from the warning process; the system would need to be as apolitical as possible to avoid any tampering of information.

In terms of operations, the system should identify possible triggering events that could result in cascading effects. It should be able to identify and connect key actors, their roles and activities. It should also be able to monitor activity in other markets and sectors (e.g. the financial markets) so as to identify how changes in one environment impact other global processes. To this end, it should also have the ability to anticipate second and third order effects.

With regard to conflicts, it would need to provide information on the motivations and interests of the parties involved, as well as highlight any deterioration in relations and possible triggers to war.

The system must be able to accommodate expertise from different sectors. It has to be capable of handling different languages and different cultural mindsets. It should enable access to rich data sources that could provide alternative analyses and a diversity of opinion, while meeting the basic normative requirements of trust, reliability and validity.

Organizationally, the system should enable innovative thinking. It should help uncover "unknown unknowns" and remedy cognitive biases. It should empower interoperability within and between the warning organization and its customers. It should draw on a truly diversified network of contacts that are well-placed, willing and incentivized to contribute.

Finally, to be of any value, a strategic warning system should allow for timely and continuous reporting.

A consensus emerged that the intelligence and warning community could best confront complex adaptive threats, such as terrorism and pandemics, by using developing a multinational, collaborative approach to warning.

A first step in this direction should be the development of common information and analytic systems. These should allow for improved knowledge sharing, metadata tagging and scenario mapping. They should also incorporate collaborative tools (e.g. wikis and electronic whiteboards) as a means of breaking down organizational walls and improving the quality of analysis on today's security issues. In line with this approach, analysts should develop a common vocabulary that can be understood by all actors working on the issue.

Access to such systems could be open or by invitation only. Either way, it should be inclusive and accommodate the views and opinions of professionals from a broad spectrum of backgrounds (public and private sector, academics, policymakers, as well as subject and region experts). Broader participation would improve knowledge of local cultures, religious practices, social norms and history. An improved analytical understanding is also possible through qualitative rather than quantitative analysis – identifying the "who" and "why" of a given situation rather than the "how" and "when".

In order for such knowledge-sharing efforts to be successful, the upper echelons of the intelligence and security community must give their full support to intra- and inter-organization collaboration and, where

necessary, incentivize and reward such activities. Flexible thinking and working are key to addressing today's threat scenarios.

Horizon scanning exercises should also be used to help identify where future threats might emerge, what form they might take, and what impact they might have on the national and international security agenda. Improved horizon scanning would enable intelligence analysts to discover new trends and understand emerging behaviors in their broadest possible context. It should also take note of economic, social and cultural issues, as well the media's coverage of these concerns.

Seminar III: Warning for Readiness in the New Threat Environment

Zurich, 29-31 March 2007

The topic of the third seminar was on factors influencing the readiness of policy and operational organizations to address potential threats. The group addressed issues such as the warning-response gap, specific needs for counter-terrorism warning, long-term foresight, and new approaches to warning and communication. The seminar series ended with a high-level roundtable discussion, looking at issues such as the relationship between intelligence and the policy process or key challenges of getting policymakers and operational personnel to act on warning.

Warning for Readiness in a Changed Environment

The group discussed three contextual factors in the international environment with significant impact on strategic warning: increasing complexity, decreasing predictability, and the changing importance of geographical spaces. Because of the changed international environment, warning is no longer about monitoring known factors with the help of stable indicators, but is also (and more increasingly) about searching for weak signals of potential, often unknown threats and risks. The importance of weak signals as indicators of emerging trends was also discussed

…most surprises in the history of intelligence have occurred due to a failure to act, not a failure to see.

While these "unknown unknowns" pose one of the greatest challenges to today's intelligence community, disputes between analysts and policymakers are usually most acute in interpreting the evidence about matters that are knowable, but not (yet) fully known to either intelligence or policy professionals. In fact, most surprises in the history of intelligence have occurred due to a failure to act, not a failure to see. The key problem is therefore often not really the collection or the lack of information per se – but consists instead of analytical difficulties, including information overload, intelligence of the wrong sort, and obstacles to warning for readiness such as psychological factors, bureaucratic-organizational factors, agenda-political factors, and others.

Additionally, participants examined the relevance of weak signals for policymakers and how new tools can help put weak signals on the radar of policymakers. Some participants wondered whether such signals might not be seen as outliers of a consensus view, especially when conducted as part of a formal exercise, such as the "future of globalization" horizon scanning exercise conducted prior to the conference.[1]

Overcoming the Gap Between Analysts and Policy-makers

Tensions between analysts and policymakers are not new but have gained additional attention since the 11 September 2001 attacks in the US. At intervals, policymakers express dissatisfaction with intelligence products or even blame them for their actions. They argue, for example, that the warnings are too vague and not actionable, or lead to warning fatigue and the "cry wolf" syndrome.

Analysts, on the other hand, feel that the policymakers' criticisms of intelligence performance are unwarranted. They object that, even though warnings have been issued, either no action or the wrong kind of action was taken. For example, some warnings are ignored despite being actionable because they are "inconvenient" (i.e. require costly or difficult adjustments) or are politically difficult to manage. Others

[1] In this online exercise, conducted immediately before the seminar, participants were asked to identify key factors that will shape the future of globalization, Using methodology developed by the Fountain Park company, participants collectively ranked the various factors, with factors judged only by a minority to be highly significant flagged as potential "weak signals" of change.

are ignored because low-tech/high-probability threats do not capture the attention of policymakers the way exotic, high-tech/low-probability threats do, despite the fact that the former should most definitely be addressed.

Further, if policy in general is focused too much on a specific and accepted threat, any attempt to deflate the threat is repeatedly thwarted and resources cannot be moved toward other concerns that have not yet fully developed. If policy officials have strong preferences or predispositions, they will mainly listen to analyses that confirm their preconceptions and dismiss the rest.

As valid as these points are, they should not come as a surprise. Warning is a human business and there is no simple input-output relationship between a warning given by an analyst and a foreseeable action on the policy level. Even when warnings are clear and actionable, organizational and systemic obstacles may result in diffused accountability or responsibility, or may magnify others costs and risks to such an extent that no action is taken. Participants also stressed the need for a history of foresight as a means of uncovering whether the warning community is learning at all, or simply repeating the same exercises without improving its performance.

Many of these grievances can be explained by lack of understanding of the other side. This is aggravated by the fact that due to the changing environment, the very nature of the "intelligence consumer" has been evolving. Today's strategic warning customer base is much larger than it used to be. Today it isn't just top-level policymakers but also state and local leaders, as well as the media and the general public that consume intelligence and influence the relationship between intelligence professionals and policymakers. As policy and policymakers become more diffuse, it becomes harder for the intelligence community to connect with policy issues. Because there is no standard definition and no "typical" intelligence customer, it is necessary to improve the understanding of each others' needs. Thus, greater emphasis on customer wishes is essential. While no single tool is sufficient to fulfill customers' requirements, what is needed is a portfolio of tools adapted to the different needs and demands of a broader customer base. At the same time, tailoring intelligence products to specific needs demands considerable flexibility on the part of the analysts.

Changing Forms of Warnings

Although the information revolution has led to the phenomenon of "information overload", more tools are available today as a result of parallel progress in technological innovation. On the one hand, such tools allow for a diversity of experience, ideas, and opinions (graphic tools, for example, could be used more widely to produce visual narratives). On the other hand, customers are now able to interact more directly with the data and thus to create more analysis on their own.

…warning must be understood as a continuous, interactive process that by its very nature calls for more interactive ways of working together.

Instead of seeing this as a negative development, the intelligence community should consider creating models, tools, or simulations that invite iterative interaction by intelligence customers. Warning must be understood as a continuous, iterative process that by its very nature calls for more interactive ways of working together. The advantage of this approach is that it would allow policymakers and other customers to persuade themselves of the integrity and accountability of the intelligence products they receive and tailor them to their needs, even though this would not necessarily guarantee better outcomes at all times, as all the obstacles to warning for readiness remain untouched by this.

Furthermore, in a changing threat environment, expertise will become more valuable if it represents the complete effort of a collaborative group that can bring greater mental resources and a diversity of viewpoints to bear on a problem. Such collaborative undertakings can again be aided by new technology and can bring in policymakers of various sorts. Examples for such networks are not only networks of other intelligence analysts working on similar issues, but can be much broader, such as high-awareness networked organizations that interlink different official actors with first-rate knowledge about the

environment and situation at hand. Even though such collaboration will force a re-evaluation of traditional warning formats, it might be highly fruitful in closing the gap between analysts and policymakers.

Participants also noted the importance of managing the expectations of decision-makers. Strategic warning is a difficult business that doesn't guarantee accuracy or success. Nevertheless, it is important that analysts develop a sense of urgency that's equal to that of their clients. They must also work harder to understand the personality of specific decision makers in order to better serve their interests and overcome traditional barriers to effective warning. Intelligence is only one input among many that decision-makers receive and the warning community must improve its ability to effectively convey its message to them.

Program Seminar 1

Friday, 10 November

8:00	Welcome Andreas Wenger, Director, Center for Security Studies, ETH Zurich Warren Fishbein, Deputy Director, Global Futures Partnership	
8:15	Plan for the Day Alain Wouters, WS Network	

Kick Off: A Practioner's View of Emerging Challenges for Warning

8:30	Speaker 1:	Ken Knight, US National Intelligence Officer for Warning
	Speaker 2:	Patrick Nathan, National Security Coordination Secretariat, Singapore
	Comment 1:	Ambassador Jacques Pitteloud, Head of the Centre for International Security Policy, Swiss Federal Department of Foreign Affairs
	Comment 2:	Nicolas Regaud, Deputy Director, French National Defense General Secretariat
	Chair:	Andreas Wenger, Director, Center for Security Studies, ETH Zurich
9:45	*Coffee*	

21st Century Challenges to Warning – The Rise of Nonstate Networked Threats

10:15	Speaker 1:	Phil Williams, University of Pittsburgh
	Speaker 2:	Kumar Ramakrishna, Centre of Excellence for National Security, Singapore
	Comment:	Aline Leboeuf, Institut Francais des Relations Internationales
	Chair:	Christian Jenny, General Secretariat, Swiss Federal Department of Defence, Civil Protection and Sports

Enduring Challenges of Warning: Cognitive Biases and Thinking Pathologies

11:30	Speaker 1:	Uri Bar-Joseph, University of Haifa
	Speaker 2:	Douglas J. MacEachin, Georgetown University and former Professional Staff Member of the 9/11 Commission
	Chair:	Roger George, Global Futures Partnership
12:45	*Lunch*	

Breakout Groups

2:00	What constitutes an effective warning system?
3:15	Report Out from Breakout Groups (5 minutes apiece)
3:45	*Coffee*

Warning Challenges for Specific Communities

4:15 Three participants from different sectors will briefly describe challenges for anticipating surprise in their areas of responsibility

Speaker 1:	Marcus Wüst, Chief Administrative Officer, Investment Banking Operations, Deutsche Bank
Speaker 2:	Ludwig Decamps, NATO HQ, Private Office of the Secretary General Policy Planning Unit
Speaker 3:	Nicholas Grono, Vice President for Advocacy and Operations, International Crisis Group
Chair:	Cho Khong, Chief Political Analyst SXE, Shell International

Program Seminar 2

Friday, 19 January

8:30	Welcome Andreas Wenger, Director, Center for Security Studies, ETH Zurich Warren Fishbein, Deputy Director, Global Futures Partnership	
8:45	Plan for the Day Alain Wouters, WS Network	

Introduction on Basic Warning Methodologies

9:00	Ken Knight, US National Intelligence Officer for Warning	

Review of Seminar No 1

9:15	Reviewers:	Josh Kerbel, Office of the Chief of Naval Operations, United States Navy Chris Pallaris, Center for Security Studies, ETH Zürich Phil Williams, University of Pittsburgh
	Chair:	Sean Costigan, Center for Security Studies, ETH Zürich

Kick Off / Keynote 2: The Unconscious and Decision-Making

10:00	Speaker:	Gerd Gigerenzer, Director, Max Planck Institute for Human Development, Berlin
	Chair:	Warren Fishbein, Deputy Director, Global Futures Partnership
11:00	*Coffee*	

Panel Session I: Warning Systems for non-traditional Threats

11:30	Speaker 1:	Stewart Prest, Senior Research Associate, Country Indicators for Foreign Policy (CIFP), Carleton University, Ottawa
	Speaker 2:	Daniel Morris, Ph.D. Fellow, Department of War Studies, King's College London (on leave from the Criminal Intelligence Service of Canada)
	Chair:	Andreas Wenger, Director, Center for Security Studies, ETH Zürich
12:45	*Lunch*	

Panel Session II: Cognitive Mapping / Sensemaking

2:00	Speaker 1:	Franz Liebl, Dr. oec. publ., Dr. rer. pol. habil., Universität der Künste, Berlin
	Speaker 2:	Dave Snowden, Cognitive Edge Pte Ltd
	Chair:	Michel Hess, Center for Security Studies, ETH Zürich
3:20	*Coffee*	

Breakout Groups

3:45	Developing a Warning Case Study
5:00	Report Out from Breakout Groups (5 minutes apiece)
5:30	Wrap-up / Adjourn

Saturday, 20 January

9:00	Plan for the Day Alain Wouters, WS Network	

Panel Session III: Horizon Scanning

9:15	Speaker:	Rupert Lewis, Head of the UK Horizon Scanning Centre (HSC)
	Discussant:	Alain Wouters, WS Network
	Chair:	Myriam Dunn, Center for Security Studies, ETH Zürich
10:15	*Coffee*	

Panel Session IV: Quantitative Models and Foresight

10:45	Speaker 1:	Joshua Sinai, Issue Consultant and Program Manager at the Analysis Corporation
	Speaker 2:	J. Scott Armstrong, Professor of Marketing, Wharton Business School
	Chair:	Luca Gatti, WS Network
12:15	*Lunch*	

Panel Session V: High reliability organizations and effective warning

1:30	Speaker 1:	Ephraim Kam, Deputy Head of the Jaffee Center for Strategic Studies, Tel Aviv University
	Speaker 2:	Karlene Roberts, Haas School of Business, University of California Berkeley
	Chair:	Pat Neary, Office of the US Director of National Intelligence
2:50	*Coffee*	

Breakout Groups

3:15	How can methodologies/concepts be applied to the case studies discussed in Breakout session 1?
4:30	Report Out (5 minutes each, filled out template online)

Plenary Discussion: Developing the GFF Forsight and Warning Community

5:00	Developing the GFF Forsight and Warning Community
5:50	Closing Comments
6:00	Adjourn

Program Seminar 3

Friday, 30 March

8:30	Welcome Andreas Wenger, Director, Center for Security Studies, ETH Zurich Warren Fishbein, Deputy Director, Global Futures Partnership	
8:45	Plan for the Day / Alain Wouters, WS Network	

Panel Session I: The Warning-Response Gap

9:00	Speaker 1:	Charles F. Parker, Assistant Professor of Government, Uppsala University, and Senior Fellow, The Swedish Institute of International Affairs
	Speaker 2:	Jim Wirtz, Professor in the Department of National Security Affairs, Naval Postgraduate School, Monterrey
	Chair:	Jan Karcz, United States Office of the Director of National Intelligence
10:15	*Coffee*	

Panel Session II: Warning for Counter-Terrorism

10:45	Speaker 1:	John Sullivan, LA Sheriff's Department, Leader of the Terrorism Early Warning Group
	Speaker 2:	US National Counter Terrorism Center
	Chair:	Sean Costigan, Center for Security Studies, ETH Zürich
12:15	*Lunch at the Hotel*	

Panel Session III: Longer-Term Foresight in the Policy Process

1:30	Speaker 1:	Alexander Van De Putte, Professor of Strategic Foresight, Geneva School of Diplomacy and International Relations
	Speaker 2:	Craig Gralley, Director, Strategic Plans and Outreach, US National Intelligence Council
	Speaker 3:	Martin Briens, Deputy Director, Policy Planning, French Ministry of Foreign Affairs
	Chair:	Martin Ortega, Senior Fellow, EU Institute for Security Studies, Paris
2:45	*Coffee*	

Plenary – Introduction to the Weak Signals Exercise

3:15	Introduction to a Weak Signals Exercise Lead: Leena Ilmola, Fountain Park Ltd

Saturday, 31 March

8:45	Plan for the Day Alain Wouters, WS Network	

Panel Session IV: Warning and Communication: New Approaches

9:00	Speaker 1:	Henry Farrell, Department of Political Science, George Washington University
	Speaker 2:	Michael Schrage, Co-Director of the MIT Media Lab's e-Markets Initiative, Senior Adviser to MIT's Security Studies Program
	Speaker 3:	Carmen Medina, Director, Center for the Study of Intelligence, Central Intelligence Agency
	Chair:	Warren Fishbein, Deputy Director, Global Futures Partnership
10:30	*Coffee*	

Weak Signals Exercise, Part I

11:00	Breakout Groups
12:30	*Lunch at the Hotel*

Intelligence and Warning Roundtable

1:45	Speaker 1:	Jorge Dezcallar, Secretary General, International Advisory Board Repsol-YPF, former Head of the Spanish CNI
	Speaker 2:	Reid Morden, former Deputy Foreign Minister and former Director of the Canadian Security Intelligence Service, President of Reid Morden & Associates
	Speaker 3:	Barry Pavel, Interim US Principal Deputy Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict and Interdependent Capabilities
	Speaker 4:	Ken Knight, US National Intelligence Officer for Warning
	Chair:	Alyson Bailes, Director, SIPRI
3:30	*Coffee*	

Weak Signals Exercise, Part II

4:00 Report Out (5 minutes each)

Plenary Discussion / Wrap Up

4:30	What have we learned/next steps
5:15	Closing Comments
5:30	Adjourn

The Center for Security Studies

The Center for Security Studies (CSS) (www.css.ethz.ch) at ETH Zurich is a Swiss academic center of competence that specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The CSS is engaged in research projects with a number of Swiss and international partners. The Center's research focus is on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy. The CSS runs the International Relations and Security Network (ISN) (www.isn.ethz.ch), and in cooperation with partner institutes manages the Crisis and Risk Network (CRN) (www.crn.ethz.ch), the Parallel History Project on Cooperative Security (PHP) (www.php.ethz.ch), the Swiss Foreign and Security Policy Network (SSN) (www.ssn.ethz.ch), and the Russian and Eurasian Security (RES) Network (www.res.ethz.ch). The Center for Security Studies is a member of the Center for Comparative and International Studies (CIS), which is a joint initiative between ETH Zurich and the University of Zurich specializing in comparative politics and international relations.

Rapporteurs

Dr. Beat Habegger, Senior Researcher, New Risks Research Unit, Center for Security Studies (CSS), ETH Zurich

Vivian Fritischi, ISN Editor, Center for Security Studies (CSS), ETH Zurich

Chris Pallaris, Head of Information Services, ISN Executive Editor, Center for Security Studies (CSS), ETH Zurich

Project Leaders

Dr. Myriam Dunn, Head, New Risks Research Unit and Crisis and Risk Network (CRN) Coordinator, Center for Security Studies (CSS), ETH Zurich

Dr. Victor Mauer, Deputy Director, Center for Security Studies (CSS), ETH Zurich

Prof. Dr. Andreas Wenger, Director, Center for Security Studies (CSS), ETH Zurich