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

## Seminar 1: The Changing Threat Environment and Its Implications for Strategic Warning

Zurich, 9-11 November 2006

CSS
An ETH Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

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

GLOBAL FUTURES FORUM

# Global Futures Forum
# Emerging Threats in the 21st Century

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

*9-11 November 2006,*
*Zurich, Switzerland*

**Organized by:**

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

## Table of Contents

# Program

## Friday, 10 November

| | | |
|---|---|---|
| 8:00 | Welcome<br>Andreas Wenger, Director, Center for Security Studies, ETH Zurich<br>Warren Fishbein, Deputy Director, Global Futures Partnership | |
| 8:15 | Plan for the Day<br>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 |

## Saturday, 11 November

| | | |
|---|---|---|
| 8:30 | Reflections on Day 1<br>Warren Fishbein, Deputy Director, Global Futures Partnership | |
| 8:45 | Plan for the Day<br>Alain Wouters, WS Network | |

### Conceptual Approaches I: Complexity

| | | |
|---|---|---|
| 9:00 | Speaker: | John Casti, Wissenschaftzentrum Wien; The Kenos Circle; The International Institute for Applied Systems Analysis (IIASA) |
| | Discussant: | Josh Kerbel, Senior Intelligence Advisor, Office of the Chief of Naval Operations, United States Navy |
| | Chair: | Helene Lavoix, Institut Francais des Relations Internationales |
| *10:15* | *Coffee* | |

### Conceptual approaches II: Viral Models and Contagion

| | | |
|---|---|---|
| 10:45 | Speaker 1: | Stephen Morse, Columbia University |
| | Speaker 2: | Paul Stares, US Institute of Peace |
| | Chair: | Joy Miller, Chief Scientist, Armed Forces Medical Intelligence Center |
| *12:00* | *Lunch* | |

### Breakout Groups

| | |
|---|---|
| 1:15 | Participants will discuss one specific challenge from all presentations, compare and contrast with own challenges, and suggest approaches for improving performance |
| *3:15* | *Coffee* |
| 3:45 | Report Out from Breakout Groups (5 minutes apiece) |

### Plenary, Table Exercise

| | |
|---|---|
| 4:15 | What key learnings do we take away from this seminar? What do we need to follow up in online conversation and at future seminars?<br>Plenary discussion, led by Alain Wouters, WS Network |
| 5:00 | Demonstration of the GFF Website<br>Jean-Louis Tiernan, Privy Council Office, Canada |
| 5:15 | Closing Comments<br>Warren Fishbein, Deputy Director, Global Futures Partnership<br>Victor Mauer, Deputy Director, Center for Security Studies, ETH Zurich |
| 5:30 | Adjourn |

# Summary of Key Issues

## Background

The Center for Security Studies at ETH Zurich and the Global Futures Forum – a multinational, multi-disciplinary, and cross-sector group formed in November 2005 at an international conference hosted by the Global Futures Partnership of the US Central Intelligence Agency – have joined efforts to conceive of new ways of thinking about strategic warning in the changing global security environment. The seminar series on Strategic Foresight and Warning is designed to help the formation of an active, vibrant, and self-sustaining community of warning experts.

Providing strategic warning to policymakers about potential threats and dangers is a key function of governmental intelligence organizations, and the one by which their performance is most stringently judged. However, the context for warning is changing as globally networked challenges increasingly overshadow their historical state-centric counterparts. The key objective of the first of three seminars was to explore new ways of thinking about strategic foresight in a significantly altered and still rapidly changing international environment. To this end, it convened over 70 intelligence experts and speakers from such fields as complexity theory, networks, cognitive biases, and forecasting, among other salient fields of enquiry.

## The Changing Environment

Three contextual factors that are responsible for the altered international environment were explored during the seminar: increasing complexity, decreasing predictability, and the changing importance of geographical spaces:

- There is *greater complexity* in the post-Cold War era: Due to the growing number of independent international and transnational actors playing power games on multiple levels revolving around national, regional, and global dynamics, the range of threats has become highly complex.
- The *level of uncertainty has increased* in the world after the end of the Cold War. Current threats are less predictable than traditional state-centric threats and come from more diverse sources: computer hackers and criminals, disaffected domestic groups, natural and man-made viral borne illnesses, and radical terrorists, including those motivated by Muslim fundamentalism.
- International affairs have become *more decentralized and regionalized* after the Cold War. More nations than previously are involved in managing international affairs, albeit often only on a regional basis. Regional issues have proliferated and threaten wider international peace and security. Non-state actors – such as terrorist groups – have taken advantage of regional conflicts and insecurities.

The changing context has substantial consequences for strategic early warning. In the broadest sense, warning is transformed from an exercise in surveillance–monitoring identified indicators (such as military mobilization) to monitor the evolution of known threats to one of "reconnaissance," meaning searching for signals of potential, perhaps unknown, threats that can emerge anywhere or at any time.

The key problem is not necessarily the collection or the lack of information – but rather analytical difficulties and challenges arising from cognitive and organizational issues. During the seminar, participants identified key challenges to effective early warning on three, at times overlapping levels:

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

### Individual level

On the first level, the delivery of better analysis is impeded by features of human cognition, by cultural biases, or by the effects of small-group processes. A solution could include recruiting and training analysts that are better equipped to deal with the cognitive challenges of information processing and analysis in the changing environment. During the seminar, participants learned that personality psychology offers methods to identify individuals with high tolerance for unmotivated biases and specific personality types that are better suited to the business of early warning. Thus, a thorough "human capital assessment" would offer prospective employers an opportunity to identify recruits with the relevant skills.

Other solutions that were discussed include the institutionalization of the role of "devil's advocate", improved 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.

### 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. Participants agreed that 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.

Participants discussed how intelligence communities will have to mimic adversaries (in terms of thinking, analysis, and organization) by learning to adapt, morph, and engage in bottom-up behavior in order to adapt to the global borderless intellectual space. A fruitful approach might be to operate at the "edge" of organizations, rather than trying to destroy old organizations or create new ones. If those "edges" could come together in collaborative workspaces, probably virtual ones, they would be the ideal. 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.

### Customer level

There was also general agreement on the need to work more closely with customers (e.g., policymakers). However, due to the changing environment, the very nature of the "intelligence consumer" appears to be evolving. Now, not only federal policymakers, but also state and local leaders, as well as the media and the public, are 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 others' needs is necessary. However, participants discussed how proactive this dialogue should be, for example when "marketing" intelligence analysis to policymakers. Some suggested that customers should be more closely involved in the business of early-warning mapping and reporting, while others believed that it might be worth looking at other models of collaboration as well as "best practices" in other countries or in other sectors.

# Foresight, Warning and the Changing Global Strategic Environment

## Keynote Remarks by Ambassador Alyson JK Bailes, Director, Stockholm International Peace Research Institute, (SIPRI)

Ambassador Bailes began with a reflection on the Cold War, when the origin of the threat to Western democracy was clear and when early warning could, at the minimum, constitute confirmation of preparations on the enemy side. Today, the greatest challenge facing the international community stems from the quantity and complexity of the threats that have emerged. These threats pose significant difficulties in terms of identification and interpretation, that in turn vary from one social group and country to another, or vary within a single nation and society over time. At a time when risks may have multiple sources, and are global in nature and linked, the calculation of risk is especially hard for a state that has several potential adversaries, and/or several vulnerabilities to attack. In addition, the risks of (and created by) internal armed conflicts must also be added to the calculation. While traditional threats can at least be geographically localized, the new threats are liable to strike anywhere and from anywhere.

Consequently, the new security environment is shaping both the language of risk (how factors of risk, risk assessment and prioritization, and the formation of policies for risk handling and response are defined) and the architecture of risk methodology by presenting analysts with the practical challenge of building a multi-risk analytical model. However, the mundane questions (what is being measured; in what setting; from whose viewpoint; and to what end) must still be addressed. Analysts increasingly must be able to manage notions of uncertainty and probability, to assess the relative gravity of impact of different events, and to judge correctly how far a public policy response is feasible and efficient. Determining the factors of connectivity (whether a type of event that can be triggered by several different causes that, in turn, can trigger multiple problems in other dimensions) should *prima facie* attract more attention and resources than assessing a risk of a stand-alone nature.

While commercial risk assessment services typically take a country-by-country approach (that lends itself to visual treatment in maps), the assessments that governments and other institutions require must elaborate the causation and consequences of major risk factors that cannot be confined to the limits of a single state. The more that important vectors are added to a multi-country analysis, the better it should help us to identify critical node points, cases of high dependency, rapid and potentially destabilizing changes in pattern, and the relative openness to risk and the vulnerability of the particular multinational community.

Ambassador Bailes further cautioned that analysts must be on guard against the subjective human perceptions and attitudes that may distort the results of analysis. Risk perceptions are skewed not only by the varying degrees to which different human risk perceptions may become combined or interact, but also by the interests and the self-defined role and responsibilities of those making the assessment. Risk assessment can go wrong when the states, organizations and interested groups fail to interact and discuss these threats as much as they should. It would be intriguing to try to compare and (where possible) combine the techniques of risk assessment and risk management used in business and other economic contexts. The broader the definitions of a modern public security policy become – especially in the fields of energy and infrastructure, public health and the environment – the more we must recognize that the private sector today is often literally on the front line, both in terms of bearing the first impact and of having the knowledge and resources for good prediction and response. This underlines how much we could gain from a conscious and cooperative blending of public and private approaches to risk, for the good of society as a whole.

## Kick-Off: A Practitioner's View of Emerging Challenges for Warning

### Ken Knight, US National Intelligence Officer for Warning

The first speaker began his presentation by reminding the participants that there are many perspectives on warning and a broad variety of views on what constitutes an effective warning system. There are no simple solutions; a broader understanding of analytical approaches that takes into account cross-sectoral and cross-national interactions is needed. While the U.S. intelligence services are under constant review (usually driven by intelligence failures) and many things have been improved in the past, effective warning still remains a difficult task.

Ken Knight outlined several crucial challenges to warning. First, he addressed the insight that warning is difficult because it deals with the futures; the issues are complex, information is often incomplete, and the stakes may be very high. Second, he claimed that there is no standard definition of warning and no "typical" intelligence customer. Many have differing ideas about what is warning, what is effective, and what is actually needed. Third, he noted that there is no majority view within the intelligence community itself on what constitutes an effective warning system. Fourth, he pointed to the time and information dilemma: the requirement to provide enough lead time to decision-makers on the one hand, but to also have enough detailed information so that, the warning is convincing. He diagnosed that analysts do not like to be wrong and tend to wait until they are certain—maybe too late. Fifth, he emphasized that intelligence is a two-way street: feedback loops and close interaction with policy-makers are crucial for a successful warning system.

In conclusion, Knight expressed the view that the pace, scale, and scope of change have increased dramatically. The interdependencies of complex issues in today's world (for instance, intended actions leading to unintended consequences) are tremendous. On the issue of information overload, he reminded the participants that analysts are inundated with data and constantly challenged to distinguish between important "signals" and routine "noise." He also noted a concern that customers of intelligence information have unrealistic expectations about what it can provide.

### Patrick Nathan, National Security Coordination Secretariat of Singapore

The second speaker presented the topic "Emerging Challenges for Warning: Singapore's Risk Assessment and Horizon Scanning Project." He began by outlining the context of the contemporary threat environment. In his view, today's threats are more difficult to predict and identify because of their rapidly evolving nature; the spectrum of challenges to national security has enlarged. There exist very disparate and diverse information sources for intelligence services and the reaction times have become relatively short. Patrick Nathan then elaborated on the strategic context that led Singapore's National Security Coordination Centre (NSCC) to set up coordinated counter-terrorist efforts: the need to prioritize scarce governmental resources, the need to put in place a coherent framework to reduce strategic surprises, and the need to focus on "low-probability high-impact" events.

Challenges to warning on a strategic level include thinking about how to make a strategic warning system relevant, how to include decision-makers, and how to get agencies across governments to participate. Challenges to warning encountered on the operational level can be clustered into three broad categories: bureaucratic (connecting silos, changing mindsets and preserving operational security), cognitive (exploiting the wisdom of the crowd and enhancing weak signal detection), and technical (sharing sensitive data, automating indexing and pattern-matching).

Nathan described how Singapore's early warning system by brings together multiple approaches and perspectives from a variety of partner organizations. A multitude of horizon scanning concepts and methods

were collected and a suite of technology tools finally used to operationalize it. He went on to explain the conceptual model of the early warning process that is now used by Singaporean authorities.

## Comments and Discussion

Two discussants reflected on the ideas presented by the two speakers. Ambassador Jacques Pitteloud, Head of the Centre for International Security Policy at the Swiss Federal Department of Foreign Affairs, concentrated his speech on several challenges to warning in the contemporary environment. The first challenge is to single out the information that is truly important and actionable. Second, he underlined the need to keep a long-term perspective. Third, he explored how risks are connected to each other and how to enable an integrated approach. Fourth, he stressed the importance of convincing decision-makers to allocate and increase resources where the real risks are (and not where the most popularity can be found). He concluded by underlining that the last point might be the biggest challenge because many of today's most urgent risks are not "popular" ones.

Nicolas Regaud, Deputy Director of the French National Defense General Secretariat, praised the Singaporean approach to early warning as a very focused and promising one because it understands early warning as a way of "filling the gaps" in national agencies. Moreover, he claimed that often it is not information, but effective work-flow that is lacking. Administrative bodies act in relatively isolated structures and are affected by rivalries between agencies, so they are not always ready to share their respective knowledge. Regaud further argued that early warning systems must be adapted to the "administrative sociology" of a country. In this context he also highlighted that essentially neither methods, tools, nor techniques matter, but what really counts is the human being: the capacity of the individual expert makes the difference – human analysis can never be replaced.

The following discussion put emphasis on the necessity of an intensified dialog of the warning community with policymakers. There was some disagreement on how proactive this dialog should be in the sense of "selling" intelligence analysis to policymakers. Some participants argued that this is beyond their mandate, which is simply to present analysis and to show possible consequences. In addition, it was argued that the intelligence community should focus more on their successes and not just on the failures. There was agreement that a successful approach needs to include multiple actors across countries and governmental structures, and that warning should not happen as a by-product of analytical activities, but always requires an intentional approach.

## Panel I: 21st Century Challenges to Warning - The Rise of Non-State Networked Threats

### Phil Williams, University of Pittsburgh

The first speaker spoke on the topic of "Early Warning for Transnational Threats." His presentation began with the proposal that practitioners step out of their daily routines and familiar methods to examine issues from a new perspective, given the changes in the new security environment worldwide. Early warning on non-state threats must provide both tactical and operational warnings. He began by discussing the need for a new lexicon for security in the new century as traditional threats are increasingly interlinked with transnational threats and have given rise to non-traditional threats.

Professor Phil Williams identified the important trends that characterize and will continue to shape the new security environment. The first factor discussed was the idea of the "new middle ages," that is the secular decline of the Westphalian state and the rise of multiple types of international actors – a period that has been termed by some observers as a state of "long-term 'durable disorder'." The second factor was disorderly spaces, areas where governance is weak or where alternatives to state governance are in place. These include zones of social and economic exclusion (as well as mega- and feral cities) that are important incubators of crime, terrorism and disease. The third factor was globalization flows (e.g. dangerous flows of illicit and elusive commodities and capital) and increased connectivity (areas with high-levels of connectivity and therefore a greater likelihood of exhibiting contagion and herd behavior, and producing cascading disruptions with international consequences).

Phil Williams identified the rise of "sovereignty-free" actors (referring to James Rosenau's work) as the fourth factor shaping the new security environment. Sovereignty-free actors are both products and exploiters of globalization, but are not constrained by sovereignty, and are better at establishing connectivity than governments, and function as distributed, adaptive learning networks that are agile, flexible, and difficult to target (in this sense superior to governments). These include transnational actors such as criminal organizations, terrorist networks, proliferation networks, and quasi-state organizations, as well as emerging and re-emerging diseases. The fifth factor included network organizations and embedded networks. He offered a reminder that network organizations are not inferior to organizations with hierarchies and may include hierarchical nodes. These networks have highly sophisticated organizational forms that make them very good at deception and embedding themselves in society and legitimate institutions. Like sovereignty-free actors, networks are also a result of globalization and are adept at exploiting it. These entities coordinate, learn and adapt, enjoying high levels of flexibility and a strong capacity for regeneration. But they also demonstrate dangerous herd behavior, and are prone to imitation and emulation as seen in organized crime, terrorist networks and the anti-globalization movement. The last factor discussed was the contextual complexity of the new security environment, which has no independent and dependent variables; rather, everything within a complex system is interdependent. Because complex systems lie somewhere between chaos and order, pattern discovery is an essential first step to understanding and managing them.

Williams concluded his talk by outlining the implications these factors will have for intelligence analysts; further noting that warning intelligence must be timely and sensitized to complexity. Analysts will need to use fresh assumptions and fresh visions of the future to engage in pattern discovery, to forge closer links with policymakers to enhance their sensitivity to the issues, and to engage in systematic probing strategies to elicit knowledge and understanding of adaptive responses. In addition, the assessment and monitoring of multiple watch-points in disorderly spaces will be essential, as will the use of open sources of intelligence and multiple indicator sets. It is important to recognize the dynamism and co-evolution of complex systems. Therefore, constant refinement and adaptation is necessary to ensure that warning itself becomes a complex adaptive system. As intelligence communities adapt to the global borderless intellectual space, in effect they will have to mimic adversaries (in terms of thinking, analysis and organization) by learning to

adapt, morph and engage in bottom-up behaviour. Essentially, the intelligence community itself will have to increase in complexity.

### Kumar Ramakrishna, Centre of Excellence for National Security, Singapore

The second speaker presented the topic, "A Singapore perspective on Counter-Terrorism Early Warning." He drew attention to how terrorist attacks in Asia shocked the region and forced the intelligence community to enlarge its early warning effort beyond the warning of imminent attacks and threats, to warning about movements within society that give rise to terrorism. To this end, the speaker offered a case study of Jemaah Islamiyah as is the key non-state networked threat to security in Singapore and Southeast Asia.

Kumar Ramakrishna offered a possible counterterrorism/early warning analytical framework that comprises five types of factors. He first outlined the contextual factors that shape terrorism, including historical elements and cultural elements that tend to shape individual and group identities. In particular, he noted that pockets of regional socio-cultural spaces that, in certain circumstances, can be conducive to radicalization. Second, the coercive elements that also shape terrorism in Southeast Asia; in particular, insensitive behaviour and attitudes (including abuse and brutality on the part of state security forces). Third, psychological and social psychological factors that interplay on the individual and group levels (such as concretist or dogmatic personalities) were also discussed. Such attitudes form the basis of religious fundamentalism (expressed as a movement that seeks to impose its worldview on others). While group identity provides distinctiveness, dignity and emotional well-being, groups are prone to accept certain beliefs. If a group perceives that it is under attack, individuals will join and support it. Therefore, a sense of group persecution reinforces the "us-versus-them" worldview and makes individuals more prone to believe their ideologies.

Ideological factors were identified as the fourth factor shaping terrorism, in particular, the threat from a radical form of Islamism, but not Islam itself. While Islam (the personal faith) seeks to transform the individual, Islamism (the political ideology) seeks to transform entire societies into Islamic states, through various modalities, including (in some variants) violence. Ramakrishna noted that in Southeast Asia, Islamism is a complex ideological phenomenon that shows a mixture of indigenous and Arab elements. The ideology of Al-Qaida is distinguished by its origins from a particular global radical Islamist movement. Al-Qaida's worldview portrays Islam as engaging in a cosmic war for survival and concludes that all Western civilians are targets because of their political and financial support (through taxes) of Western governments. The fifth factor identified was comprised of socio-economic and political elements including marginalization in the region. This circumstance combined with a lack of access to education and a lack of employment opportunities promotes a general sense of dissatisfaction that allows radical ideas to take root and provides opportunities for extremists exploit.

He concluded that the transnational, networked non-state threat of Jemaah Islamiyah arises from the specific conjunction of localized contextual factors and psychological/social psychological variables, and is influenced by the specific ideological factor of Al-Qaidaism and radical jihadist ideologies. Ramakrishna emphasized the need for a counterterrorism, early warning framework that focuses on area studies research and highlights "bottom-up" not "top-down" analyses that identify the important contextual, political, socio-economic, historical and cultural "root causes" of local Muslim alienation. He further recommended the psychological profiling of key Muslim leaders and probing of communities of concern to detect evidence of concretist, categorical thinking and to determine of how much radical worldviews have been adopted and adapted.

### Comments and Discussion

Aline Leboeuf (L'Institut français des relations internationals, IFRI) served as commentator to the discussion. In particular, she identified as the most significant problem facing the intelligence community is how

to identify and manage the new threats, and how to bridge strategic thinking on an operational level. Contrary to previous speakers, Aline Leboeuf emphasized that that the world is not necessarily more complex than it was during the Cold War. She cautioned that an ongoing discourse about the chaos of the new situation is dangerous for it engenders passivity and biases in analysis (which ultimately may create the risk of unforeseen impacts and unexpected consequences) that are not compatible with making sense of the new security environment.

She added that it will be important to recognize (and understand as far as possible) both identified and non-identified threats. She suggested the intelligence community might wish to reconsider the establishment of concrete profiles, given that such networks tend to change so rapidly. She also noted the simplest method may be to break down the threat by units of analysis, such as network actors, linkage actors, states, non-state actors, passive supporters, groups and individuals, while distinguishing between connected insiders and disconnected outsiders. Leboeuf further cautioned that globalization has also given rise to a rapid process of individual technological empowerment. Early warning will have to determine how long it may be before single individuals hold significant destructive capacity and strategic goals.

There followed a lively discussion regarding governed and ungoverned spaces, the activities and goals of various networks, as well as how states might react and adapt to the changing security environment and the advent of the "new middle ages".

## Panel II: Enduring Challenges of Warning: Cognitive Biases and Thinking Pathologies

### Uri Bar-Joseph, University of Haifa

Professor Uri Bar-Joseph focused his talk on the topic of "Improving the Intelligence Process: A Different Approach." He began his presentation by quoting Sun-Tzu's dictum that if you know your enemy and you know yourself, you need not fear the battles ahead. In the current security climate, however, Bar-Joseph asked whether we know ourselves well enough to address the security challenges we have to face. There is a consensus that the main reason behind most intelligence failures is not insufficient information but rather the incorrect interpretation, understanding and processing of this information.

He spoke of Operation Barbarossa, the attack on Pearl Harbor, the Korean War, the War of Yom Kippur, and the invasion of Afghanistan by Soviet forces as just some of the "surprises" of recent history that can also be attributed to a failure of intelligence. These failures can generally be attributed to three different sources, one on the individual level is the problem of cognitive dissonance, heuristic judgment, and confirmation bias; the second source on the group level stems from the problem of group think; and, lastly, on the organizational level there is the rejection of new information that is inconsistent with existing preconceptions.

Bar-Joseph went on to outline some of the means by which these problems can be overcome or, at the very least, reduced. These solutions include the institutionalization of the role of "devil's advocate"; improved mechanisms of information flow; improving the formal education of the intelligence analyst; professionalizing the analyst's job; and implementing ethical standards for analysts. Although such "fixes" have been suggested before, the fact is that after 40 years of effort and the recent intelligence failures surrounding 9/11 and the WMD pretext for the invasion of Iraq, the shortcomings of existing intelligence agencies are still valid. In both of the above cases, the failure was due to a failure of imagination and a rigid adherence to existing preconceptions.

Bar-Joseph went on to outline other problem areas where a change of approach is necessary. To begin with, at the root of the problem are unmotivated biases that obstruct the flow of information. Attempts to overcome these biases typically fail. The impact of such biases varies from individual to individual, making a collective approach to the problem difficult. That said, personality psychology offers methods to identify individuals with high tolerance for unmotivated biases and intelligence organizations can use these methods to select and promote such analysts in order to minimize their effect on the analytical process.

What's needed, therefore, is not a change of system but rather a change of analyst, one better equipped to deal with the cognitive challenges of information processing and analysis. There are two ways of selecting such analysts. The first method is known as the "five factor model" which measures extroversion, neuroticism, agreeableness, conscientiousness, and openness to experience. (This last point refers to the individual's willingness to explore, consider and tolerate new and unfamiliar experiences, ideas and feelings.) The second method examines the individual's need for "cognitive closure" or rather the desire for a confident judgment on an issue as compared to individual comfort with ongoing confusion and ambiguity. Individuals demonstrating such behavior seek closure as quickly as possible and keep closure for as long as possible. The other behavioral traits of an individual with a need for cognitive closure are: a poor appreciation of novel perspectives; a rejection of opinion deviates; a denial and reinterpretation of inconsistent information in terms that match one's prior conceptions; an insistence on clarity, order and coherence; considerable self-confidence; and an authoritarian style of leadership and decision-making.

Uri Bar-Joseph concluded by asserting that in the recruitment or promotion of intelligence analysts, it is essential to measure to what extent they need cognitive closure. Far more attention needs to be given to an individual's openness to new ideas and new approaches. This is a key determinant to overcoming the indi-

vidual biases that obstruct information processing. However, openness alone is insufficient. More attention must also be given to the need to nurture cultural expertise (and not just in the form of language skills), build balanced analysis groups, and maintain institutional memory and expertise.

### Douglas J. MacEachin, Georgetown University and Member of the 9/11 Commission

Douglas MacEachin's presentation focused on "Why Personality is also Important." The speaker began by following on from Bar-Joseph's comments and insisting that intelligence analysts should not be selected simply on account of their educational backgrounds. If a potential recruit answers "no" to the question of whether they want to have a successful career in the intelligence service they should be chosen over those who answer "yes". He went on to argue that the problem of intelligence failures will not be addressed until those working within the intelligence community realize that they are human and subject to mistakes, weaknesses and cognitive biases. As such, it is important to build into the intelligence profession those practices designed to protect analysts from themselves.

When it comes to gathering and processing intelligence, in-depth research on a given topic is just as important as the immediate news. The failures arise not when analysts refuse to "go beyond the evidence" but rather when they fail to identify the evidence. Most failures have their root in a single premise in the logical argument. (e.g. "the Shah of Iran can't possible be toppled from power as he has all the military power he needs," or "the Soviet's will not be foolish enough to invade Afghanistan and thus sacrifice détente"). All intelligence is a work in progress. Analysts must learn to adapt their approaches to collecting, synthesizing and interpreting intelligence information. This would allow for a more nuanced interpretation of the intelligence problems that analysts face. Conducting an intelligence analysis on a single premise is unwise, regardless of whether it is based on an empirical evidence or expertise.

MacEachin went on to describe how different "vectors" and "drivers" influence the intelligence process. Thus, it is important not to "predict" what will happen but rather to describe the forces shaping a given situation. In other words, what would happen if new vectors and drivers were introduced or existing ones modified? In conducting such an exercise it is essential to collect as much information as possible and then try and figure out what is happening and why. Surveys and assessments, the scanning and tracking of different factors, the proper consideration of different stimuli, responses and results – all should be examined carefully before assessments are made and conclusions drawn.

He argued that in all instances the basis of the dominant premise should be uncovered. This can be done by simple deduction, going down the list of possible reasons for the existence of the premise until it has been uncovered. But how does one deal with the premises of policymakers? After all, the principal premise is often in line with the policymakers view. The answer here lies with the limits of the intelligence community's responsibilities. MacEachin argued that the business of intelligence was the truth, the whole truth, and nothing but the truth. Anything beyond that is for the policymakers to contend with.

A few comments followed on the qualities of an ideal intelligence officer. Echoing Bar-Joseph's comments, MacEachin argued that an attitude to openness is essential, although cultivating such an attitude and new mental models can sometimes be difficult. There was no "strategic picture" in place to alert the intelligence community to the possibility of an attack on the scale of 9/11; as such, an attack did not fit the mental models of the day and information suggesting something was imminent did not flow.

### Comments and Discussion

Roger George, Global Futures Partnership, served as commentator to the discussion, offering insight into how people learn to process information. In particular, George discussed how mental models are created as individuals grow and adapt, and why they are difficult to change. He also reminded participants that culture encourages and rewards members for neither reframing nor reevaluating, and suggested that the intel-

ligence community must acknowledge the problems it faces and work toward solutions as part of a new professional ethic. Such an approach would need to change the current institutional professional ethic that rewards junior analysts and reinforces the culture of the organization.

The discussion that followed focused on the challenges of identifying underlying premises and reducing cognitive bias in analysts. Participants also considered the role that managers could play in halting the premature shaping of premises by analysts on the individual and group levels, as well as ways the intelligence community can begin to protect itself from bias.

## Reporting on Breakout Groups, First Session (10 November 2006)

In the afternoon, the plenary group was divided into five breakout groups. The input of the morning sessions was used for discussing a very practical question: Given the changing international environment, what constitutes an effective warning system? The groups were arranged to identify a variety of critical success factors before selecting the two most critical ones for reporting back to the plenary.

The first group suggested a solid two-way communication system between analysts and decision-makers that starts with an improved understanding of each others' needs and includes the implementation of different approaches for building communities and integrating them into institutional structures. Another critical factor is horizontal (across government) and vertical (across multiple actors) information-sharing.

The second group opted for a warning system that is small, flexible, adaptive, resourceful and on-top of changes in the environment. The overall objective of a warning system is to enable informed action. For this, the analysts need to have a clear understanding of the customer and the customer's needs; while the customer should be more willing to accept a certain degree of fuzziness in the presented analyses.

Group three proposed understanding early warning systems as "fluid networks" rather than as organizational entities. They also emphasized better conceptualizing the warning mission in order to distinguish it from intelligence, and reiterated the call to think through the relationship between the provider and the recipient of early warning.

The fourth group focused on the need to provide enough lead time for mitigating risks. On the individual level the appropriate framing of methodologies is crucial; the managerial level is responsible for constantly reviewing the methods and adapting them to a changed environment; and on the level of policymakers, it is essential to set up a permanent dialogue with the warning community.

Group five underlined the importance of direct access to decision-makers and a procedural setup that allows for good communication between analysts and political leaders. They also suggested an interactive "warning education" to enable the customers of early warning need understand the process and challenges, and be able to express to analysts what they actually want to be warned about.

## Panel III: Warning Challenges for Specific Communities

### Martin Wüst, Chief Administrative Officer, Investment Banking Operations at Deutsche Bank

Martin Wüst, Chief Administrative Officer, Investment Banking Operations at Deutsche Bank, described the typical challenges facing an investment bank; provided an overview of potential threats and interruptions to work processes; and explained how the bank acts to mitigate emerging risks and improve warning by connecting available information.

Wüst outlined the four primary operations of international banks (that of capturing trades, loan operations, securities and derivatives), and noted the risk to international banking operations stems from the fact that Deutsche Bank conducts some 60,000 trades per day. Therefore, risks and threats to information technology are among the most significant issue of concern.

While Deutsche Bank faces the classic well-managed risks, such as counter-party risk, it also faces systemic risk (associated with markets, failure of large banks, changes in liquidity payment flows), operational risk (stemming from data input errors, information technology errors, corporate security, fraud, terrorist attacks and hacking), catastrophic risk (from pandemics, hurricanes and tsunamis), and man-made catastrophic risks that have knock-on effects (such as large-scale terrorist attacks). In addition, the bank also faces risk from interruptions in critical banking operations that may stem from critical IT failures that cascade through system. These include critical information technology failures occurring outside the bank, for instance in the Asia-Pacific region, or, for example, a telecom outage in Stockholm, as well as critical power failures occurring where critical clearing institutions are located.

While the banking community watches for such warning signs in areas of importance, it also must appraise and anticipate risk with regard to information systems capacity, such as anticipating the effects of communications and power infrastructure systems reaching peak capacity—the bank tries to offset this risk by setting in place systems of redundancy. In addition, the bank watches for evidence of successful penetration by adversaries (such as members of organized crime, disgruntled employees, and, in some countries, state employees) and interruptions stemming from complex externalized events. These would include police instituted traffic and crowd controls for international meetings (such as the WTO meetings) or, other major public events (for example, during the 2004 Republican National Convention in New York, in which barricades limited bank employee access to offices).

Like other institutions, banks assess risks by type and category. Risks such as natural hazards are relatively easy to anticipate, whereas new risks require the adoption of new warning signs. The failure to anticipate risks is a reflection of the failure of imagination, rather than failing to have adequate information.

### Ludwig Decamps, Policy Planning Unit, Private Office of the Secretary General, NATO Headquarters

The second speaker presented on the topic of "Challenges for NATO" and the consumers of strategic warning and foresight. NATO's corporate governance is largely comprised of processes, customs and decision-making processes governed by consensus. Consensus is both important and problematic for the development of organizational strategic foresight on issues of concern, as some member-states question whether such activities should exist at all. As it stands, NATO has no information collection capacity and no military. It relies on the resources made available to it by its members.

Ludwig Decamps asserted that such difficulties highlight the fact that there needs to be a greater link between the warning intelligence community and the policy community. There needs to be a means for linking the key imperatives of both communities together. The real challenge for NATO is to have greater linking, coordinated planning and the development of strategic foresight. Both the policy and intelligence

communities suffer from bias and have the tendency to view things from their own environment and perspective. The organization's tendency is to focus on immediate payouts and results rather than long-term gains, and to be overly-focused on structures that are reinvented for each problem.

It would be used to employ tools aimed at building strategic foresight, to develop scenarios, to build on predictions and projections, to link ideas, and to move from linear to adaptive planning. There is an increased acceptance on an organizational level that more integral planning is necessary. There also needs to be a more holistic approach acting on different levels in the physical, informational and cognitive domain. It should be directed toward issues of importance and a timely response that observes, orients, reacts and schemes. The intelligence community should adopt methodologies for scenario-based early warning and should establish more network-enabled capacity.

### Nicholas Grono, Vice President for Advocacy and Operations, International Crisis Group (ICG)

The third speaker, Nicholas Grono, focused on the early warning and the "Challenges of Anticipating Conflict." From the perspective of people working in the area of early warning in the field, he explained, the problem isn't early warning, but early response. In the case of Rwanda in April 2004, there was significant evidence that planning for large-scale violence was underway. The response on the part of the international community to early warnings was to begin removing troops. In terms of early warning, failing states present a threat not only to the region where they exist, but also to the world.

Grono argued that early warning should lead to early action, but noted that in the case of international organizations, obstacles to taking decisive early action are created by the very members whose states sustain the greatest risk. For instance, the UN secretariat, which has 16 to 18 peacekeeping missions comprising some 100,000 troops, has only 157 staff members dedicated to planning. It has no substantial early warning system because of member state resistance. While NATO, which has three missions, has approximately 1,000 planning staff available. The ICG seeks to have analysts in or near areas to identify underlying political, economic and social conditions that provide early warning of civil conflict. Cultural understanding is vastly improved by having regular reporting from people in the field.

The ICG warned the international community about Afghanistan, and other field-based analysts (such as Sydney Jones) warned about the Jemaah Islamiyah in Southeast Asia, and that others warned US payments to preferred leaders in Somalia would result in a public preference for the nascent Islamic courts. Though the ICG's primary customer is the general public, it does work with other warning communities, and works to shape policy or advocacy by aiming to reach policymakers and meet with desk officers. The ICG employs UN workers in the field who cannot give certain reports internally.

The weakness of current analytical frameworks in shaping early warnings is that they overly focus on the quantitative aspects of information; while NGOs often focus on the qualitative factors underlying risk. The two primary qualitative models, greed and grievance (now called "feasibility vs. motivation"), should be better integrated into risk analysis. The greed (feasibility) model (advanced by Paul Collier), considers the influence of economic factors and conflict; that is, how factors such as low per capita income and the economic incapacity of states lead to a decrease in recruitment costs for radical movements. The grievance (motivation) model focuses on the religious and ethnic factors that give rise to risk, in particular evidence of inequality and political instability. While regime type is a dominant determining factor of stability, the role of democracy factors in ultimately shaping the regime type. Thus there should be constant focus on the risks of conflict.

## Comments and Discussion

Commentary was offered by Mr. Cho Khong, who cited a well-known study by Philip Tetlock on expert political judgment and noted that the more famous the expert, the worst their track record in forecasting tends to be. Why do experts have this problem? An analyst without much expertise is much more likely to go through and examine each aspect of the information available, while an expert is more likely to draw broad extrapolations based on their expertise and experience with a given subject. However, with regard to organizations and analysts, the lack of readiness to admit where policy was wrong blocks improvement of the system. Perhaps those who analyze trends are less suited for creating warnings. In early warning the decisive factor is whether or not such warnings will be acted on.

In the retrospective, scenarios must be seen as having predicted well, or to have directed thinking in the right direction. The intelligence community needs to build in network capabilities and holistic approaches to connect what it knows and what others know. There needs to be a willingness to listen to a wide-range of debate before deciding on the outcomes and actions to be taken. It is important that movement is made before a conflict erupts. For instance, the ICG Monthly Bulletins (summaries of developments over the month) come from places where there is no active conflict. The ICG has to deal with the "dog that doesn't bark" warnings, that don't give immediate and obvious results. Perhaps there is a need for adapted scenarios, and for the scenario development process to be made more dynamic, more open to pathways other than those suggested by existing scenarios.

## Panel IV: Conceptual Approaches 1: Complexity

### John Casti, Wissenschaftzentrum Wien, The Kenos Circle, The International Institute for Applied Sciences

John Casti spoke on the topic "Complexity, Emergence and the Flow of Events: Why We See the Events We Do - And Not See Something Else." He began his address by arguing that many of the problems faced by today's intelligence agencies are the result of complex, adaptive systems such as stock markets, road traffic networks, evolutionary and agricultural systems, and national economies.

There are four distinguishing "fingerprints" to such systems: space, agents, information and interaction. John Casti gave the example of a football game to clarify these fingerprints further. The "space" is the playing field; the "agents" are the players; "information" is drawn from the behavior of nearby players; and the "interaction" is drawn from the blocking, tackling, kicking and other activities of the players. John Casti went on to elaborate on the three key fingerprints of complexity and complex systems. To begin with there is always a medium-sized number of agents. This number can vary, but it is always between a few dozen and a few hundred thousand.

Second, these agents are intelligent and adaptive, although not intelligent as a cognitive psychologist would understand the term. Instead, they use rules to operate in a system and decide what to do on the basis of these rules. They are adaptive in that they can change the rules as they wish. Unlike in the world of physics where rules don't change, in the social and behavioral domain the agents involved are always changing the rules. Consequently, you also need "meta-rules" or rules for changing rules.

Third, these agents operate according to the local information available to them. No single agent or object is aware of what every other agent is doing. All decisions are thus made on the basis of partial information or local knowledge derived from a smaller information space. No decision is possible based on complete information. John Casti gave the example of a commodities trader who, by working closely with an associate in Hong Kong, knew more about this colleague then he does about the person sitting next to him.

One of the most important features of a complex adaptive system is the display of "emergence" and "emergent behavior". It is not possible to identify emergent behavior by focusing on a single agent in the system. Financial markets are one example of emergence and emergent behavior in practice. Here all decisions are gathered and their emergent properties are made manifest in the form of price changes. The price of a commodity doesn't change as a result of one individual trader but rather through the interaction of all.

Casti followed these comments by elaborating his theory on the decline and fall of globalization. He argued that while globalization meant different things to different people, the popular interpretation advocated by the journalist and author Thomas Friedman is in decline. To explain why, he introduced the theory of "socionomics". This theory argues that the collective social "mood" in a population (whether global or otherwise) creates or causes a climate within which certain types of behavior are more likely to happen than others. This mood will, in turn, determine the outcome of future events. Casti warned against imputing our individual thoughts and behaviors on entire groups. The dynamics and laws of group behavior are different to those of individual behavior. The social climate created by a group gives rise to certain kinds of actions and behavior that tend to have a qualitatively different character. Thus, when asking a group how it feels about the future, the logical response may well be: "Which future?" A "sociometer" thus becomes a means by which the mood of the population can be measured. Again, financial markets are a good way of measuring social moods as they reflect the bets people are making about the future at all time scales.

Actions and events have characteristic time frames and are indicative of the social moods of their time. Casti gave the examples of the post-World War II bull market and the "Skyscraper Index" as examples of positive social moods in action. Skyscrapers, such as the Petronas Towers in Malaysia, are usually built at a

time of national optimism or confidence. By the time construction has finished the national mood had typically soured.

By this measure, Casti argued that globalization – which is the result of a generally increasing, positive social mood around the globe – has also reached its peak and is due to decline as time goes by and the mood turns negative. To illustrate his hypothesis, Casti presented several slides demonstrating the fortunes of globalization against post-war global markets, the publishing industry's appetite for books on globalization, and the number of anti-globalization articles in the media. He noted that there is a strong correlation between social mood and anti-globalization sentiment around the globe. A similar parallel can also be seen in the fate of the EU. Casti noted that the EU was born from a post-War desire to overcome traditional enmities and benefited enormously from the positive social mood surrounding its birth. Now, its fortunes are in decline together with social opinions on its value. As a result, we may yet see a reversal of sovereignty back to individual European states.

Casti ended his presentation with a series of points to consider. First, mathematics and computing do not equal magic. Second, with regard to complex, adaptive systems, it is feelings and beliefs that matter and not deductive rationality. Third, one must appreciate that group behavior and not individual feelings or actions determine the course of events. Fourth, agent-based models serve as laboratories for controlled, repeatable experiments. And fifth, Ross Ashby's law of requisite variety that argues that "only variety can destroy variety."

### Comments and Discussion

Commentary was offered by discussant Josh Kerbel, Office of the Chief of Naval Operations, United States Navy. Kerbel first highlighted a maturing appreciation of the discipline of complexity. What was once a technical issue is now being appreciated as a cognitive one. The faddishness associated with complexity during the late 1990s has been replaced with a serious post-9/11 need to think about thinking. Kerbel agreed that the fingerprints of complexity are all over the global system. Their existence gives rise to a number of non-linear behavioral corollaries. First, a complex, adaptive system is not equal to the sum of its parts. These systems change disproportionately according to their inputs and outputs at varying times. This presents cognitive challenges to people working in intelligence. Moreover, such systems cannot be reduced (or understood) by analyzing it. Second, one has to accept the inevitability of unintended consequences. And third, one has to appreciate that the element of timing really matters.

Kerbel went on to argue that in order to address these corollaries what's needed is a synthetic perspective of the system and an interdisciplinary socionomics, as all issues are affecting each other. An analysis of a country's military strength, for example, cannot ignore political or economic factors. Furthermore, the inevitability of unintended consequences also undermines the flat world theory. Multiple feedback loops are in play—second and third order effects can alter initial assumptions and expectations. These factors defy simple trend analysis; nice neat story lines simply won't do as they ignore other factors. Finally, with regard to timing, it is important to recognize the many factors, conditions and trends that come into play and create the mood by which an action is possible. Intelligence analysts therefore need to think pretty far ahead, especially as scenarios are not static.

How does the intelligence community address these challenges? A good first step is with the help of cognitive changes. Analysts should search for better models, adopt the use of biological and medical metaphors (e.g. "side effects", "contagious idea", etc.), and learn to work with visualization tools that can aid with understanding complexity. Kerbel went on to suggest that what the intelligence community needs is both analysts and synthesists. These synthesists would compliment the regular analytical process 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.

## Panel V: Conceptual Approaches II: Viral Models and Contagion

### Stephen Morse, Columbia University

Stephen Morse spoke on the subject of emerging and re-emerging viruses and opened with a discussion of the major viruses that have occurred in modern history, including the Black Death (1348), which destroyed one-third of the population of Europe; small pox, which killed more than all historical wars combined; and cholera, which killed 0.5 million in the United States and 50 million worldwide in two years during the 19th century, as well as the 1918 influenza virus.

Presently, in much of the world, infectious diseases remain the major cause of disease and death. Among these are the forgotten (re-emerging) infections such as diphtheria, that reappear when neither funds nor personnel are available to keep up immunization programs, and emerging infections (not previously recognized) that rapidly increase in incidence or geographic range, these have anthropogenic causes that are important factors in the disease's emergence.

The epidemiological "host + agent + environment + vector" model is the hallmark of infectious disease transmission via respiration, sexual, vector-borne (e.g. via mosquitoes, oral, food and blood-borne) pathways. Emerging infections are rapidly increasing in incidence and geographic range. (These include AIDS, which introduced new mechanisms that were poorly understood.) Changes in the world environment have also facilitated the rise of novel diseases whose impact under these conditions cannot be predicted. What we do know is that anthropogenic causes have the greatest influence on the spread of these novel diseases. The result of human activities provides new pathways to a larger population where the disease can establish itself. (For instance, SARS was rapidly transmitted across the globe via air transportation and the Avian flu may also infect the world more quickly because of these new pathways.)

Syndromic surveillance is one of most important tools used in monitoring disease emergence. In the past, syndromic surveillance was limited to analyzing disease signs and symptoms, using non-diagnostic data and other automated systems. Today, disease surveillance includes emergency call, hospital emergency room visits, data from pharmacies and records of employee absenteeism that are used to determine if there are significantly more calls for flu-like or other unusual syndromes. In the case of the West Nile virus, a doctor in New York City noticed the unusual symptoms and cases. In pharmacies, the monitoring of acute increases in prescriptions for antibiotics or sales of over-the-counter cold remedy drugs is also important. Public health networks, such as ProMed Mail (www. Promedmail.org), which is a moderated listserv that averages 7 medical reports per day) play a vital role in surveillance and monitoring, and can significantly boost the monitoring of traditional health reporting.

### Paul Stares, United States Institute of Peace

The second speaker addressed the application of viral models and contagion to terrorism analysis and warnings. Like viral models, early warning seeks to identify those who are infected, those who are susceptible, and those who have been removed from the infected population. The Classic viral models, which include the "SIR" model and the epidemiological triad, could provide useful analytical frameworks for terrorism analysis. The "SIR" model identifies the "susceptibles" or the pool of potential recruits, and activists), the "infectives" (supporters, proselytizers and militants), and the "removed" those killed, captured or "immunized" and "rehabilitated". The epidemiological triad identifies the host, the agent, the environment and the vectors through which the infection spreads. An epidemiological approach to early warning provides the following benefits, in particular systemic/multi-dimensional analyses and the development of intelligence processes and frameworks that are dynamic and evolutionary. This approach is analytically adaptive and promotes empiricism.

Paul Stares went on to argue that what's needed is a "conceptual leap" and an application of these viral models to emerging threats by monitoring the spread of information or ideas with pernicious effects. In particular, the surveillance of incidents of communal violence and political instability, financial contagion and economic instability, the emergence of organized crime, humanitarian disasters, and terrorism (both as a movement and its activities). Here too, the language of epidemiology is frequently used by analysts and commentators. Al-Qaida, for example, is said to have "infected" others with its ideology. Although there are differences and similarities with disease surveillance and early warning, both provide over-the-horizon risk assessments, strategic warning indicators on the regional and local levels, and can give rise to an intra-global research surveillance network.

Stares concluded that much as the medical community fights instances of disease, those actors fighting terrorism and other such risks should seek to remove the most critical or virulent nodes for these are the ones with most influence. This would prove much more effective than treating and attacking all nodes as if they were identical. Counterterrorist policies should make more of an effort to prioritize and differentiate the critical nodes.

## Comments and Discussion

The two presentations were followed by a discussion of the potentials for using health care responses such as immunization, disease eradication, containment strategies and the protection of high-risk elements of society (by adopting remedy to address background conditions) to model the intelligence community's response to terrorism and crime. The participants also discussed the role of networks as "superspreaders" and the potential for identifying other spaces (such as prisons and madrasas), key individuals and activities that also enhance superspreading. In addition, the participants explored the importance of gaining a better understanding of how ideas move thorough populations, possibilities of using ideological inoculation strategies to expose to jihadist messages and undermine them. In all, the participants agreed that strategic warning of the emergence of disease is essential for tactical warning to be timely and effective.

## Reporting on Breakout Groups, Second Session (11 November 2006)

Considering the discussions of the first seminar day, four critical challenges for strategic warning had been selected for more thorough discussions in the Saturday breakout sessions. These challenges were organization, sense-making, policymakers, and assumptions. Each participant was asked to join one of these groups. Their common purpose was to discuss the selected challenge, to relate it to one's own experiences, and to suggest approaches for better understanding and addressing it.

The first group on "organization" admitted that the legacy of the US early warning system as a quite successful one during the Cold War makes it difficult to change it today. The principle of US intelligence – that every analyst is an early warning analyst – bears the risk that it confers responsibility upon everybody and thus ultimately responsibility rests with no one. They suggested creating a "culture of vigilance" within decentralized environments, but with permanent focal points that enable coordination, communication, outreach, quality control, etc. They also proposed the creation of more creative and experimental structures and a culture of learning from mistakes.

The second group on "sense-making" had difficulties clarifying this term and finding a consensus among group members. They stressed the ability to cross-reference contacts, self-critique and self-review, and intuitive thinking for sense-making. They also highlighted encouraging a process of asking questions, exploring and understanding aspects of mass crowds, and the importance of building teams within organizations.

The third group discussed "how to best serve policymakers?" and examined the often strained relationship between providers of analysis and their clients. In view of the warning product, the obvious question is how to tailor it to the client's needs. A subsequent question then is how neutral can it be if it is intended to provide useful guidelines for policymakers. With respect to possible ways of intervention, it is essential that analysts understand the needs of policymakers. Each product must be delivered according to the client's needs and a well-tailored process may often be more important than the product itself.

The fourth group on "assumptions" dealt with the question of how to identify and potentially adapt assumptions in a rapidly changing environment. They emphasized the unique challenge of enabling an organizational culture that constantly challenges institutional processes and human mindsets. It is extremely difficult – although urgently needed – to challenge the assumptions of what we know, what we understand, and how we act. One possible method of intervention is to bring in people from the outside tasked with deliberately challenging assumptions. Another approach might be the public sharing of intelligence analysis in order to let it be challenged by the general public.

## Plenary Table Exercise and Closing Comments

The close of the conference offered participants the opportunity to express their views regarding insights, lessons learned and future activities. What follows is a summary of the comments made.

### Lessons Learned

More than one delegate commented on the value of attending a conference that brought together a wide-range of agencies, experience and approaches. There was also general agreement on the commonality of concerns and the institutional and bureaucratic challenges shared by the delegates.

Clearly, the business of early warning is a difficult one to which there are no easy solutions. One delegate commented on the importance of learning more about how these actors modeled the risks they identified, either through practical exercises or further discussion.

There was also general agreement on the importance of cultural change within the intelligence community, in particular with regard to accommodating different cognitive approaches and organizational "mavericks" and skeptics who aren't afraid to think differently and communicate bad news. The private sector could be one place to look to for lessons on implementing successful cultural change while NGOs could offer useful advice on cultivating radical thinking.

Delegates also agreed that although the intelligence community makes it a habit to learn from its failures, it doesn't invest much time into learning from its successes. This should change.

### Follow-Up and Next Steps

With regard to follow-up activities, delegates recommended landscaping and mapping the different tools, techniques and approaches currently used in the field of early warning. A practical demonstration of these tools and techniques would be very helpful indeed. One delegate suggested taking a particular challenge and having the representatives of different early warning systems demonstrate how they would work through this problem or other case studies.

It would also be interesting to see how different national organizations have used their early warning systems to deal with the problems they have identified. It was further suggested that the Global Futures Forum continue the discussion on sense-making, including where and how it is being used and what tools are available to support it. It was also noted that many intelligence agencies are still struggling with semantics and definitions. What's urgently needed is a lexicon of basic terminology that can be used by all early warning actors.

There was also general agreement on the need to work more closely with customers (e.g. policymakers). Some suggested that more effort should be made to understand their needs and expectations, while others thought that they should be more closely involved in the business of early warning mapping and reporting. The more practical questions must also be answered in order for early warning to be more properly appreciated by policymakers and others: Why does the intelligence community do warning at all? What exactly is it trying to warn about? How should it "sell" or deliver its findings?

Participants agreed that it is also important to look more closely at the cultural and cognitive factors that inform the work of early warning. If possible, it would be helpful to create a catalog of best practices in early warning that takes into account the diversity of approaches. Furthermore, how does the intelligence community train analytical techniques? Who should be trained in these techniques and how? Is there a specific personality type that's better suited to the business of early warning? What skills do you need to have in order to prosper in early warning? A thorough "human capital assessment" would be appreciated here as it would offer hiring managers an opportunity to identify recruits with the relevant skills.

Follow-up activities should also address the "tracking and scanning" dilemma. One delegate noted that there is a difference between the reconnaissance and surveillance aspects of early warning. Once a threat has been identified, how should the intelligence community track and scan its evolution? To use a policing analogy, there is a different between "walking a beat" and doing a stakeout.

Finally, it was noted that early warning is not just about identifying threats but also opportunities. Future activities should also make more of an effort to explore these opportunities and to see how they can be exploited for maximum effect.

The conference closed with a demonstration of the GFF website by Jean-Louis Tiernan of the Privy Council Office in Canada and concluding comments from Warren Fishbein, Deputy Director of the Global Futures Partnership, and Victor Mauer, Deputy Director of the Center for Security Studies. Both men thanked the participants for coming to the GFF and for their contribution to the discussions.

## 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 NATO and the Warsaw Pact (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 the 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 Chief 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 at the 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