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

Seminar 2: Sense-Making and Warning -
How to Understand and Anticipate Emerging Threats

Zurich, 19-21 January 2007

Global Futures Forum
Emerging Threats in the 21st Century

Seminar 2:
Sense-making and Warning –
How to Understand and Anticipate Emerging Threats

18-20 January 2007
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, 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

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.

The focus of the first symposium was on historical and contemporary challenges in strategic warning, drawing on the literature in such fields as complexity theory, networks, cognitive biases, and forecasting, among other salient fields of enquiry. The second of three seminars built upon the theoretical foundations presented in the first seminar and focused on methodological approaches for establishing early-warning systems. It referred to concrete methods, instruments, and tools; presentations were delivered on cognitive mapping, horizon scanning, quantitative models, and other methodologies.

Traditional Warning Methodologies

Monitoring and surveillance methods for tackling traditional threats define a set of indicators and a possible timeline towards the escalation of a conflict. Once a (large) set of indicators has been established, a warning signal emerges as soon as an indicator passes a certain level. The analyst does not analyze the data in the strict sense of the word, but feeds significant amounts of collected information into the system. Although these indicator-based approaches are always 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 main weakness of this method, however, is that the 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.

Weak Signals, Sense-Making, and Warning

The concept of strategic early 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 which will constitute a strong trend in the future or can have dramatic consequences. Usually, five stages are distinguished during which weak signals mature and become strong signals: 1) the weak signal emerges. At this stage, something just "feels funny", but it cannot be pinned down. Usually this is confirmed only by a hunch or occasionally stray pieces of data; 2) the source of threat becomes known; 3) the shape of threat becomes concrete; 4) the response strategies are understood; and 5) the outcome of response can be predicted.

Clearly, these various stages require different approaches. 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.

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. The scanning itself relies primarily on examining various media sources, private-sector "gray literature", and websites, using the technique of content analysis.

Furthermore, the cognitive sciences have demonstrated that human intelligence is based on pattern recognition: This means that people think in patterns and not in streams of logical thought. Therefore, weak signals can be detected most easily by taking advantage of our brain's pattern-matching capabilities. 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 similar 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.

Inevitably, therefore, no single analytical technique can be rated as the most accurate approach to the study of all problems, so that analysts must apply the methods that are best suited to a given problem and consider combining approaches when possible 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.

Early-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. This requires analysts with good expertise, strong language skills, an extensive cultural understanding, and access to rich data sources that can provide alternative analyses and a diversity of opinion. 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 a lack of participation of potential future users in the implementation phase, a lack of joint understanding of the nature of "weak signals", differences in system requirements that may be concealed by various interested parties, excessive reliance on alleged "hard data", a lack of interaction among users, and finally a lack of integration with the strategic functions of an organization. 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 challenges posed by the structure of the intelligence community and to demolish the walls between data analysis and collection, intelligence and operations, and within intelligence organizations themselves.

What Are the Threats in the 21st Century and How Do We Respond:
The Case for a Strategic Approach

Keynote Address by Dr. Rudolf Adam, President, Federal College for Security Studies, Berlin

Rudolf Adam began his speech with a quote from Mark Twain who said that all predictions are very dangerous, particularly those in relation to the future. Indeed, the future is and will remain unpredictable. A main contributing factor is the unstoppable progress of human knowledge. Another one is that even if we knew what lies ahead of us, we would still need to generate the political will to act upon this knowledge. It is always easy to dismiss the warning by arguing that predictions may in the end turn out to be empty or that the danger might go away by itself. Adam called this the "hope despite knowledge" syndrome for "hope" has always been the stronger political factor than knowledge. Risk perception is highly irrational, it is usually colored by emotions; personal risks are perceived very differently than public risk. What is therefore needed in dealing with risks is a systematic and patient process of generating public awareness in order to cultivate enlightened communication about risk and threat perceptions. Different individual experiences and assessments need to be pooled in order to arrive at more balanced and adequate judgments. Further, good risk analysis requires salesmanship to convince, mobilize and win support for the necessary action.

An examination of the history of the 20th century prompts the questions, "Where are we heading now?" and "What does the future hold?" Adam suggested that threats and risks will be much more diffuse than in previous periods. The Cold War, with its bipolar security structures, is over. The world of the 21st century will be multipolar. Maybe less so in military terms, but economically, socially and culturally it will be less Western-dominated than the 20th century. Yet, we know relatively little about the new actors. How will China, Russia, India, Brazil and the Arab or the African worlds define their ambitions, their roles and their interests? What is certain is that neither China nor India will transform themselves into replicas of European or North American societies and that they will also have their share of problems.

Adam identified a variety of pressures that characterize the new global landscape. First, increased pressure on commodities will result in rapidly rising real costs. Second, the pressure to contain the effects of climate change will increase. Third, social pressures and the widening divisions within and between nations will result in disaffected people becoming radicalized. Fourth, growing population pressures will result in increased illegal and uncontrolled migration. Adam went on to elaborate on the proposition that the 21st century will be one of nuclear proliferation. Between two nuclear centers only one relationship exists, which lends itself easily to concepts of balance and equilibrium. The process of arms control and disarmament builds on such easy relationships. However, with seven nuclear actors creating 23 relationships, it will be much more difficult to establish the necessary degree of transparency and trust, to measure aggressive potential and defensive needs and to factor hostile intent. Reducing the problem to a question of proliferation is insufficient and a dangerous illusion. The setting is completely different from the Cold War. The logic of "mutual-assured destruction" does not hold anymore because there are nuclear protagonists who simply cannot accept a first strike and nuclear neighbors that have no meaningful warning times. With the possible exception of Israel, no state's existence is under military threat today. So, the important question to ask is why are nuclear weapons being maintained and what threats are they intended to deter?

Another threat is the turning of the tide in the global energy market, which is transforming from a buyers' into a sellers' market. The world reserves of fossil fuels are concentrated in an area stretching from the Arabian Peninsula north to encompass the Caspian region directly north to Western Siberia. In this so-called "strategic ellipse" over 70 percent of the global oil and gas reserves are concentrated, furthering the power of OPEC and, in particular, the power of countries such as Russia, Turkmenistan and Iran. Today,

already some 75 percent of the global oil and gas reserves are nationalized. Thus, it would be naïve to believe that the international energy market functions according to the liberal model. In the future, energy may not only have a price denoted in dollars, but may also carry a price in political concessions. The threat is not that oil wells physically dry up, but that we may find ourselves sitting on huge reserves of fossil fuels that are inaccessible for political reasons. Adam therefore suggested focusing less on the exhaustibility of supplies, but on their accessibility and the political stability guaranteeing their access.

What can be done in view of the volatile, fluctuating and diffuse threat situation? First, the solutions have to be as flexible, fluctuating and adaptable as the nature of the threats. Adam proposed developing resilient, multi-purpose security structures, avoiding high degrees of specialization, remaining open and – above all and foremost – sharpening the intelligence community's analytical capabilities. The better we are informed about what might happen tomorrow, the better we can arrange our defenses. He suggested building up intelligence by sharpening analytical tools, gathering relevant data from which to narrow down the likelihood of future events, and working to improve decision-makers' susceptibility to such analyses.

His second recommendation was to develop strategic thinking, which requires a hierarchy of goals, a clear analysis of the environment, a long-term commitment and a clear understanding about the resources and means required to achieve these goals. Strategic thinking anticipates future developments and takes the necessary measures today in order to be in an optimal position tomorrow. This also requires an understanding of psychological factors, a feeling for social, technological and environmental change, and the ability to remain open for change and innovation. Strategic thinkers focus on the main goal, but remain undogmatic, open-minded, self-critical and absolutely precise in the assessment of the reality. Further, empathy and the ability to see the world with other people's eyes is fundamental. Strategic thinking begins with models and assumptions about the future and the better we can map the landscape of the future, the better we will find our way, and the easier it will be to occupy the strategic zones that reinforce our strengths and competitive advantages.

Kick-Off: The Unconscious and Decision-Making

Prof. Dr. Gerd Gigerenzer, Director, Max Planck Institute for Human Development, Berlin

Dr. Gerd Gigerenzer began his talk on the topic of "The Unconscious and Decision-Making" with anecdotes illustrating that intelligence is a thing of the mind. The security officer, for instance, who picks the right criminal out of a large crowd at the airport without any physical descriptions to aid him only knows that he must look for someone who is "looking" for him and intuitively makes the right decision. Another example is the successful CEO who is not able to tell why he always makes the right decisions. At least part of his success, he admits, might be due to his "gut feelings". The lesson here is that many human decisions are not based on quantitative reasoning or systematic methods, but on intuition.

Intuition is a judgment that appears quickly in our consciousness, whose underlying process is unconscious, but is strong enough to act upon. According to Gigerenzer, the underlying process of intuition is neither an optimal weighting of all reason, nor is it a divine voice, a sixth sense, or just a lucky guess. It is rather based on what he calls "fast and frugal heuristics." These are strategies that focus just on a few important characteristics and ignore the others. A few examples may help to illustrate this proposition.

Harry Markowitz, the famous economist and Nobel laureate, based his private investment decisions not on his complex economic optimization model, but relied on a simple heuristic: he allocated his money equally to each of N funds (1/N). Empirical tests showed that the simple 1/N-model was superior to any other investment approach. The reason might be that no parameters are weighted and therefore no estimation errors – which can distort the model's predictive accuracy – occur. Although the 1/N-heuristic certainly does not hold in every situation, it is well-suited when the predictive uncertainty and the number of N is large and the learning sample is relatively small.

Another example is the large difference in organ donations between neighboring or culturally and socio-economically comparable countries. In France, for example, 99.9% of adults are organ donors, but in Germany the number is only 12%. No rational explanations apply, but a simple heuristic provides the answer: the level of donations depends on whether the legal system establishes an "opt-in" or an "opt-out" framework. If the organ donation participation is to be increased, changing the regulatory framework would be much more effective than any information campaign or other public relations activity.

A key advantage of intuition is its robustness. This is due to its tendency to simplify things if something is difficult to predict. Empirical experiments show that a reliable predictive model needs to display a certain complexity, but not too much. Usually neither the simplest nor the most complex model does best: a fairly simple model outperforms both. When laypeople and experts were asked to pick German stocks, laypeople relied on intuition: they tended to pick stocks from highly recognized companies and achieved high returns, while experts opted for less known stocks and lost money. Another example is the emergency room where quick and reliable decisions are needed. While physicians often rely on their intuitive judgment or the very complex assessment tools that use a large number of predictors, empirical evidence proves that both approaches are outperformed by simple heuristics. In this case a three-step decision-tree with three simple questions that have to be answered "yes" or "no" is used. This is more complex than the physician's situational intuitive judgment, but less complex than a model with 57 predictive indicators.

Gigerenzer further pointed to five popular misconceptions about heuristics. He stated that we do not rely on heuristics only because of our cognitive limitations; people do not use heuristics only in routine decisions of little importance; optimization is not always better and heuristics do not necessarily produce second-best results; more information and computation is not always better; and security is more than a technological problem. He concluded by outlining a few key lessons: first, if forecasts fail, do not

automatically add information – consider deleting information; second, experts can fail by thinking too much; and third, simplicity, transparency and trust are crucial.

Comments and Discussion

When asked how to develop simple heuristics of one-off events such as major terrorist attacks, Gigenzer replied that there are no such events. There are always past examples to draw on for the one real important task: to teach people that it will happen again and to anticipate possible future events now. He further said that when deleting information in order to build reliable decision-trees, the crucial factor to keep in mind is the order in which to ask the questions. Both steps are essential: to determine the adequate questions, as well as to ask them in the right order.

He also advised to analyze the situation first and then decide on the predictive model to be used. Analysts need to be taught for what purpose complex models are best-suited, and in what situations they should rely on heuristic thinking. This choice also depends to some extent on the analyst's experience: for experts it might be better to go with their "gut feeling" than for novices. However, no studies to date have examined the potentially different intuitive capabilities of different people, except for one study that could not find significant differences between men and women.

Panel I: Warning Systems for Non-Traditional Threats

Stewart Prest, Senior Research Associate, Country Indicators for Foreign Policy (CIFP)

Mr. Prest began by outlining the mandate and activities of the Country Indicators for Foreign Policy (CIFP). The aim of this initiative is to provide Canadian policymakers with real-time analytical data that identifies the related risks that fragile states face. It also provides policy relevant diagnoses on the impact of aid policy and decision support tools and guidance for policymakers. Prest outlined the structural data methodology. The indicators draw on NGO reports and other sources of information to predict the fragility of a state.

Prest then introduced the concept of state fragility and the implications for development and foreign policy as demonstrated by the data collected on fragile states. He argued that authority, legitimacy and capacity result in a functional state. A non-functional state, however, lacks one of the above elements. A fragile states therefore lacks the functional authority to provide basic security, the institutional capacity to provide basic social needs, and the political legitimacy to effectively represent their citizens at home and abroad.

In particular, Prest noted that some 20 analytically distinct terms are used to describe fragile states; this variety makes policy coherence difficult, for every organization and agency can find what it believes is important and may be motivated to pursue independent efforts that may not improve the overall situation on the ground.

By providing these tools to enhance the assessment of an event and the effectiveness of policy, CIFP aims to assist in the evaluation of when to intervene / engage or withdraw from a fragile state (e.g. by noting countries where promoting democracy has a negative impact on the fragility of the state).

Daniel Morris, Department of War Studies, King's College, London (on leave from the Criminal Intelligence Service of Canada, CISC)

Daniel Morris's presentation focused on the efforts of the Canadian government to create an early warning system on organized crime for the law enforcement community. Organized crime generally has five characteristics that are relevant for early warning: it is transnational, clandestine, networked, adaptive and connected (participates in a global network and the global economy). The challenges inherent in warning of this threat stems from the asymmetry of vulnerability, the wide "signal-to-noise" ratio, and the 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.

The CISC's approach to strategic warning of criminal activity was to build a strategic warning capacity – an effort that went through several phases. First, a research phase that included outreach to specialists and a feasibility study. Then, the development of a basic methodology that was used to build pilot products that were later refined. On the basis of these results, the methodology was reevaluated and publicly published to generate debate and feedback. From this process new warning products were then created and a national program to build the network by training warning analysts regionally around Canada was implemented. One of the new products is the Sentinel Watch List, which provides contextualized, practical and up-to-date information on threat prevention and perception over time. This service is regularly updated and encourages greater information-sharing.

This was conceptualized as a bottom-up, analyst-driven approach to early warning that begins with threat perception, moves on to the development and evaluation of threat scenarios, and finally to the creation of a basic indicators list that is used to assess the level of threat. Law enforcement officers are an important link in the process, as is observing and projecting trends in the threat environment. In creating this

network, the CISC learned that warning is a different type of analysis that requires a different approach and skill set. The challenge of warning stems not from a problem of collection, but of analysis. In addition, it has been important for the CISC to know its audience, collect feedback, and provide tailored assessments.

Comments and Discussion

The session was followed by an active discussion on fragile states, where participants noted that the most important aspect of monitoring and assessing fragile states comes not from a calculation of economic indicators, but from an assessment of the degree to which a central government is not functioning. The assumption that state failures are an anomaly contradicts the fact that for many people states are an artificial construct and collective structures (such as tribes) are more compelling. What is important is that those who provide aid have an understanding of where their efforts can have a positive impact and what the trade-offs are.

The participants then discussed the challenges CISC faced in implementing this criminal warning system given the significant shift from traditional warning processes. The decision to restructure the process was both top-down and bottom-up: a manager had a vision that appealed to senior decision-makers, and the analysts were tasked to develop the process.

While all early warning systems tend to identify key individuals who are suspect and then follow their personal connections, an interesting notion that goes against conventional counterterrorism wisdom is to follow the resources and money. The environment scans for criminal warning employ an unstructured approach that uses, for example, news reports, private sector "gray literature" and websites. The "unknown-unknowns", however, are managed using speculation and scenario-building that aim to anticipate how organized crime may try to exploit a novel situation.

Panel II: Cognitive Mapping / Sensemaking

Franz Liebl, oec. publ., Dr. rer. pol. habil., Universität der Künste, Berlin

The title of Dr. Liebl's presentation was "Managing Ignorance: The starting point of strategic marketing." According to Liebl, the basic problem of strategic marketing is that managing knowledge is managing ignorance. In the field of strategic marketing, managers face unmanageable consumers and various stages of unpredictability. Dr. Liebl referred to the work of Paul Schumacher who identified the four classes of knowledge when facing the future: (1) the things we know; (2) the things we don't know; (3) the known unknowables; and (4) the unknown unknowables. In strategic marketing, managing knowledge entails four strategic areas (methods) that transform the terrain of knowledge. Understanding the consumer's world (and how one is perceived in the market) is the starting point for developing innovative products and for achieving a competitive advantage. The customer's world is shaped by their perceptions, experiences and feelings. One approach, access marketing, can help managers develop ideas and probe consumers / customers to see how they react, make sense of their behavior and how they perceive new environments. This process can also help detect unknown attributes of meaning to the consumer.

Another method is to collect consumer narratives about how they use a product and to learn how products are experienced, which allows the identification of misappropriations (or rather customer-driven product innovations). From this information the manager can also identify novel segmentation criteria and customer expectations. Traditional survey questions may not reveal important unknown variables. Cognitive maps can also reveal new customer experiences and expectations. Framing is also an important tool, but can be problematic when no frame is available. The methodology of managing ignorance in strategic marketing draws from many fields, including the cognitive sciences, cognitive mapping, ethnography, anthropology, and the sociology of knowledge, among others. It also employs two approaches for sense-making: making sense of novel environments and products, and probing activities and the reservoir of framing.

Comments and Discussion

The presentation was followed by questions regarding cognitive mapping as a part of marketing and the use of weak signals to indicate market-share. In such cases, customer narratives can reveal information about the customers and their use of the products that traditional satisfaction surveys do not. Customers cannot be managed; it is not possible to optimize or make precise forecasts and customer behavior may change so rapidly that optimization models may be obsolete. As such, the old approach of "predict and prepare" should be abandoned for more modern approaches to understanding customers. Context-rich information on customer behavior is more important for strategy, and trends are less important than the conditions that create them. Liebl added that it's not enough just to collect data on such topics; it is also important to look at the context. Similarly, it's not enough to look at trends but also at the conditions that foster them.

Dr. Dave Snowden, Cognitive Edge Pt., Ltd.

Dr. Snowden focused his presentation on naturalizing approaches to sense-making. He began by defining a naturalizing approach as thinking and practice based in the natural sciences, in particular in complex adaptive systems theory and the cognitive sciences. Naturalizing means working with things the way they are, without adopting an idealistic view of how they should be – a bottom-up system design. In sense-making the traditional assumption is that "right data" leads to "right decisions," but this gives rise to three problems: Do we see the data? If we see it, do we pay attention? And if we do pay attention, will we act or can we get another to act on what we see? Each problem must be handled differently.

A science-based approach to sense-making draws on the cognitive sciences and the fact that human intelligence is based on pattern recognition: the human brain runs information through patterns that exist in the long-term memory. People don't make connections when information doesn't match previous patterns.

As such, pattern-based intelligence is the filtering of data between prior patterns and reacting accordingly. As Snowden explained when scanning data only a tiny percentage of one's visual range is in sharp focus, but the brain fills in the gaps. In the West this rate can rise to 5 percent and in the East (and in other in symbolic language structures) up to 10 percent. This process of pattern recognition can give rise to missed patterns or "weak signals" which we don't see because we don't expect them. In a complex system, where the number of possible connections can be very high, the ability to see is overwhelmed with possibilities (for example, four points have six possible linkages and therefore 64 possible patterns). This explains why, as in the case of intelligence warning prior to 9/11, people have difficulty connecting the dots and making sense of the information they receive. A naturalizing sense-making approach aims to maximize weak signal detection in a complex system.

Snowden outlined several methods to accomplish this, including the application of the Cynefin framework which can enhance sense-making. 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). He also discussed conducting large-volume narrative capturing, in which data is indexed using common metadata tags which are later analyzed for emerging patterns. These narrative-based assessments can identify some 20 percent of weak signals.

Snowden also suggested moving away from structured interviews, questionnaires and hypothesis-based research because they generally impose some bias. Instead stories about experience should be collected, tagged and the metadata from tagging analyzed for patterns. Risk assessment in horizon scanning can be approached similarly, using sense-making items such as stories and pictures. These can also be tagged and analyzed for patterns. He also addressed the possibility of using probing (to see what patterns are possible), safe-fail environments, retrospective coherence and boundary models to understand complex adaptive systems, but noted the limits of applying traditional risk management approaches to systems that are complex and chaotic.

Comments and Discussion

The presentation was followed by a discussion of the approaches to probing (in particular, leaking data to see how populations respond). Field operations are best-suited to constructing probes that can be presented as messages or field interactions. Several participants inquired about the presence of bias in data-tagging. Dr. Snowden explained that it is not possible to eliminate bias, especially if people do their own tagging. He highlighted four types of tagging and the benefits of each approach: filter tagging, which provides measurements with opposing negatives on a scale (e.g., "too patronizing – too child like"); multiple-choice questions to identify why a story was told; direct questions in pre-hypothesis research that ask about the story told (rather than directly for the story); and the identification of keywords in a story that are then matched to the storyteller.

Breakout Groups: First Session (19 January 2007)

The first round of breakout groups were given the task of understanding and outlining (where possible) the requirements of a transboundary warning system. In particular, they were asked to identify the needs and requirements that would have to be met in the case of specific warnings. The participants were divided into groups that explored the specific warning challenges of the changing face of terrorism, India-Pakistan relations, high energy prices, the ascendancy of the Shia in Iraq and the Avian flu (see Appendix A).

Shia Ascendancy in Iraq

The report from the breakout group focusing on the ascendance of the Shia in Iraq began with a caution about the complexity of the problem, the number of unknowns and the unpredictability of known players. The warning system should aim to identify these and the possible triggering events that could result in cascading effects. Such a system should aim to avoid failing to define and share its objectives upfront and should aim to remove politics from the warning process. The system would need to be as apolitical as possible to avoid any tampering of information. The group recommended that the system also emphasize understanding of the culture and education of the Shia sects. These efforts should be supplemented with effective monitoring of key areas (energy structures, infrastructures, and functional country sectors), defining of key actors, and identifying the roles of coalitions. It will be important to determine if the warning system is an open or closed system and how it should operate. The group 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.

Sustained High Oil Prices

The group reporting on high energy prices recommended a transboundary warning system that focuses on trends and developments among the oil exporters, in the political realm and in financial markets that could impact, shape, or drive the energy market. The group suggested an effort be made to determine (to the extent possible) the unknowns in these areas. The requirements of this warning system would include monitoring the investments of the various key market players (especially their activities in the Futures markets to establish what their strategies may be) and examining the fungibility of sources (in particular information about extraction sources and the factors that determine oil pricing). The system should also monitor activity in the currency markets, shifts such as an acceleration or delay of resources, subtle changes in standards of living, and political activities that may be precursors of rising energy prices. Overall, the group felt that because there is a greater likelihood of losers than winners in this scenario, the system should also consider the broader implications of rising energy prices.

The Changing Face of Terrorism

The first group report was on the changing face of terrorism. While the participants aimed to define the concept, they found limitations in doing so and focused on providing warning on terrorism. The group felt that understanding the conditions for emergence would be a main objective. Efforts should be made to bring to light the environment in which terrorism emerges and identify potential targets – thus fulfilling the warning function. However, they cautioned that doing so would introduce the additional risk of losing face when an event fails to materialize. The system requirements for a transboundary warning system include the need for good expertise, strong language skills, an extensive cultural understanding, and 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. The group also addressed the importance of

meeting basic management issues: such as identifying customers, seeking a consensus among concerned parties, creating an environment tolerant of diversity, and enhancing and sustaining interoperability and innovation.

India-Pakistan

The group reporting on a potential India-Pakistan conflict found that a transboundary warning system would need to highlight any deterioration in relations potential, critical events and changes in the possibility of war. The system would also have to provide information on motivations and the red-lines on both sides (including the "where" and "how" of India's pressure on Pakistan), while providing objective risk calculations and trajectories. Such a system would have to draw on a truly diversified network of contacts that are well-placed, willing and incentivized, and able to monitor and report on critical information as well as be provided with such information. The group highlighted the importance of creating a network with a degree of shared purpose and the ability to cater to the need for timely and continuous reporting. The group cautioned, however, that there were real concerns about how tasks would be organized and managed in such a network. Would it have a central control mechanism or a server (enabler) function? Should the approach be active or passive? Would this network engage in probing? The group also noted that a shared purpose or mission statement could be necessary.

Avian Flu Outbreak

The group reporting on the establishment of a transboundary system on the Avian flu faced a slightly different challenge as the scenario's basic assumption was that a human-to-human transmissible strain of the virus was already spreading. As such, the function of this warning system would be first to determine the quality of information about a disease outbreak – the network could use probing to clarify knowns and unknowns. Because the Avian flu is a diffuse threat that requires global cooperation, the network would meet a common need and have a shared purpose, but it would also face significant challenges given the threat's cross-discipline and cross-geographic nature – interoperability would therefore be an important concern. The group felt another major function of this transboundary system would be to provide warning to mitigate the effects of the disease vectors, especially of cascading secondary and tertiary effects (riots, other mass behaviors and the impact of dread risk). This information should also be shared with the private sector. Overall, the group recommended building scenarios to anticipate such risks and to ensure that good risk communication is done. However, there was some concern as to whether this was an appropriate function of the system, although all agreed it must be done by some party.

Panel III: Horizon Scanning

Dr. Rupert Lewis, Head of the UK Horizon Scanning Centre, London

Dr. Rupert Lewis spoke on the topic of horizon scanning and first described how the UK Horizon Scanning Centre (HSC) was set up a few years ago. Structured interviews with horizon scanning strategists from a broad range of industries helped to extract the barriers and enablers of successful horizon scanning. A variety of key success factors were determined: the purpose of horizon scanning and the organizational processes must be clear; it should meet the real needs of the clients; concepts, messages and communication should be kept simple; civil servant engagement and senior level buy-in are essential, and strong analytical capabilities (tools and techniques) must be available.

According to the definition provided by the UK Chief Scientists Advisers Committee, "horizon scanning is the systematic examination of potential threats, opportunities and likely developments including (but not restricted to) those at the margins of current thinking and planning. Horizon scanning may explore novel and unexpected issues, as well as persistent problems or trends." From this definition a useful business model was then developed around three main questions: What is horizon scanning's value proposition? What capabilities are needed? Who endorses the project?

The HSC was launched in March 2005 with the mission to inform strategic issue prioritization and to help others to raise their own capabilities. The idea of horizon scanning is to look ahead: beyond the usual timescales, beyond the usual sources and beyond organizational boundaries. It does not predict a single specific future, but focuses on the implications of (many) possible futures for today's decision-making. Those participating in a horizon scanning exercise should look at opportunities, as well as threats, and focus on areas of uncertainty and disruptive influences. A good horizon scanning approach enables both the resilience and adaptability of public policy strategies. It must be linked to strategic planning so that the research / scanning process and the implementation of the results are integrated into the public policy process.

The HSC developed two specific horizon scanning tools. First, the Sigma Scan (Σ Scan), which scans the work of others and synthesizes it into a database in order to create global horizon scanning evidence. The database is not designed to be comprehensive because it is not possible to include every subject and concern, or to set up an all-inclusive list of categories. Second, the Delta Scan (Δ Scan), which gives a complementary perspective of about 250 scientific experts in order to take stock of the state-of-the-art, as well as future trends and developments of many scientific disciplines. Both scans can be publicly accessed over the internet (www.sigmascan.org, www.deltascan.org).

Horizon scanning is not something new. It has already been applied in many parts of government. What is new, however, is that it is done explicitly; it is systematically built into government processes and is part of the management training for public servants. Some people thought and still think of horizon scanning as a form of crystal ball-gazing. Therefore, it is very important to create a good reputation for horizon scanning exercises in order to gain credibility with decision-makers and public servants. The HSC is forced to be client-oriented because it has no authority over any other government agencies. Consequently, the process of engaging with clients is tremendously important. Communication is a key success factor for horizon scanning in order to continuously reinforce why it is important and why it contributes to effective public policy-making.

Comments and Discussion

The subsequent discussion focused on Lewis' experience in establishing the Horizon Scanning Center and convincing government agencies to participate in such exercises. Lewis admitted that for some organizations or agencies, horizon scanning would not prove beneficial. Everything depends on the environment people were working in and the issues they wish to address. Some organizations active in horizon scanning have concluded that by identifying new issues or areas of concern and marketing their existence, they were able to generate more interest in their work. In attempting to overcome organizational resistance to such exercises, Lewis and his team must often identify where the power lies in an organization and work to convince this key individual or group.

The discussion ended with the admission that no matter how rigorous a horizon scanning exercise might be, people should still plan for and expect "wild cards" in real life. No scenario can be perfectly anticipated.

Panel IV: Quantitative Models and Foresight

Dr. Joshua Sinai, Issue Consultant and Program Manager, The Analysis Corporation

Dr. Sinai's presentation was titled "Forecasting Terrorism Using Quantitative Methods: A Practical Model." He began by arguing that successful forecasting is only possible if you have defined the problem you hope to confront. To this end, he defined terrorism as "[a] tactic of warfare involving premeditated, politically-motivated violence that is perpetrated by sub-state groups against any citizen or state, whether civilian or military, in order to influence government policy by causing casualties and physical destruction."

Sinai went on to assert that frequent events (e.g., terror attacks in Israel) are easier to predict than rare events (e.g., terror attacks in Western Europe or North America). Nevertheless, it is still possible to forecast a terror group's tactics, the type of attack they are likely to carry out, and the steps required to launch the attack itself. Forecasting, after all, is a probabilistic assessment focusing on general trends. Naturally, one has to be prepared to deal with the elements of randomness and surprise. But an effective forecasting model is a tool that can be adapted and refined as necessary. Effective forecasting requires an awareness and appreciation of the steps and components needed to mount an attack. The greater this awareness, the easier it is for the counterterrorism community to plan, develop and deploy an effective response, identify likely terrorists and uncover plots.

Sinai introduced different analytical methodologies to enable improved forecasting. The first, geo-spatial predictive analysis, is an attempt to predict the location and date of future terror attacks by accumulating data on a group's previous incidents and their geographic locations. To this end, data is fed into a software application that generates threat signatures such as trends in tactics, techniques and procedures. Using a geographic interface, this system is then able to identify terrorist hot-spots. As with all predictive systems, it has its limitations: it only considers successful attacks and not aborted operations or failed attempts; insight from high frequency areas isn't necessarily applicable to rare event regions; and it focuses on *incidents* rather than on *people*, which limits its ability to predict terrorist behavior.

The second technique involves data mining technologies. Here, large volumes of data on known and potential terrorists can be harnessed and analyzed using data mining tools to identify links and patterns in different data repositories, identify anomalies and predict which individuals are likely to carry out terror attacks. Data mining tools complement HUMINT and SIGINT surveillance and can help identify key players and their communication tendencies. However, it is still difficult to identify meaningful patterns in large streams of data and it does not enable effective information-gathering on unknown individuals. Because identifying terrorists is harder than identifying suspicious consumer behavior, the approach can generate false positives.

A third technique employs a project management-based approach. Terror operations can be characterized using a project management model with tasks, schedules and lines of responsibility, for example. Understanding this model enables the counterterrorism community to delay or disrupt an imminent operation, conduct "what if" analyses and guide the systematic search for evidence. Unfortunately, the model also relies on a limited set of technical indicators rather than complementing technical factors such as the characteristics of groups and the nature of their leadership.

The fourth technique is based on social network analysis. This incorporates, correlates and visualizes biographic, religious, demographic and other social data, and identifies the networks of connections and relationships between individual actors, enablers or groups. This approach enables one to understand why individuals become radicalized and how they are actually recruited. (Most terrorists, Sinai added, are drawn in through social bonds. This explains why young, educated Muslim men who are disaffected often become radicalized.) Unfortunately, social network analysis, while important, does not complete the big

picture.

Sinai concluded that the tools and techniques available to assist the work of terror forecasting are no substitute for effective human intelligence. Instead, they facilitate education, analysis and operations. With forecasting, there is no magic bullet; the best approaches combine several methodologies and synthesize strategic, operational and tactical intelligence. Dr. Sinai ended by counseling forecasters and analysts to expect randomness and to understand that the past is not always the best predictor for the future.

Professor Dr. J. Scott Armstrong, Professor of Marketing, Wharton Business School

Dr. Armstrong's presentation was titled "Methods for Predicting Decisions in Conflict Situations: An Application of Evidence-Based Forecasting." Armstrong began by arguing that predicting how people will respond in conflict situations – what decisions they will make and what actions they will take – is one means towards improved conflict forecasting.

Armstrong presented the results of various studies on conflict forecasting. Particular emphasis was given to the accuracy of opinions given by experts and non-experts alike using different analytical methods to predict the outcomes of different conflict scenarios. The scenarios themselves were modeled on real-life events.

He explained that the "unaided judgment" method was the most commonly used for predicting decisions in conflict situations. This method is most appropriate when experts are unbiased, large changes are unlikely and the relationships between the conflicting parties are known. With this method, the expert community was more likely to make an accurate forecast of how a conflict would be resolved. A second method explored the effects of experience and "time spent" on the accuracy of forecasts. A third approach considered the accuracy of game theorists. With both approaches, the unaided judgment was again more likely to be accurate.

Armstrong went on to explore the use of structured analogies in forecasting (e.g. comparing the current conflict in Iraq to the Vietnam War). In this instance, however, the use of structured analogies led to improved forecasting and predictions. Clearly, if people are familiar with an analogy they tend to better predict how a conflict might evolve.

Armstrong then considered the impact of role-playing as a means of understanding how different parties might behave in a conflict. Surprisingly, however, this approach did not lead to improved forecasting. However, the use of simulated interactions – a form of role-playing in which an administrator describes the target situation and the protagonists' roles, and then provides a list of possible decisions – reduced forecast errors significantly. Studies that have analyzed combining the two approaches, simulated interactions and structured analogies, found this increased the level of accuracy to approximately 88 percent.

Finally, the success of prediction markets as forecasting tools was also considered. Prediction markets are shaped by the aggregated opinions of hundreds (if not thousands) of individuals, all predicting (or betting) on the likelihood of a future event. This approach, commonly referred to as the "wisdom of crowds", has been known to result in accurate forecasts although the results are skewed when people are given the wrong information. Armstrong ended by summarizing the different approaches and argued that a combination of different forecasting tools should be applied when trying to predict the outcomes of different conflict situations.

Comments and Discussion

The questions that followed focused largely on the different forecasting methodologies used to predict terrorist attacks. Dr. Sinai stressed again that methodologies varied according to where and how they were being applied. Inevitably, no single analytical technique can be rated as the most accurate approach to the study of all problems, analysts should continue to apply methods best-suited to the given problem and to consider combining approaches when possible in order to maximize the accuracy of results.

Panel V: High Reliability Organizations and Effective Warning

Dr. Ephraim Kam, Deputy Head of the Jaffee Center for Strategic Studies, Tel Aviv University

Dr. Kam opened his presentation with a description of the activities and responsibilities of high reliability organizations that provide early warning in Israel. These structures must first provide warning against a conventional attack. This has resulted in organizations with a rigid / inflexible conception and a lack of openness. This makes it difficult for them to assess an enemy's intentions and gives rise to other important obstacles. Second, these structures must provide warning against terror attacks, strategic suicide bombings (that aim at mass casualties) and weapons of mass destruction. Warnings of suicide bombings are difficult given that preparations are not visible and only 3-5 people are generally involved. Small groups such as these can move easily, blend into local populations, are difficult to penetrate, and don't require extensive preparations for an attack. These structures must also warn for peace, that is to define early warning indicators for peace. Finally, high reliability organizations must warn against the collapse of key regimes.

High reliability organizations face challenges posed by the structure of the intelligence community. These organizations must determine where the responsibilities and borderlines for early warning are situated while facing walls between organizations that place restrictions on the transfer of information and create lags in the transfer of critical information to operational levels in real time. In real time, this problem is worsened by communication difficulties between those who provide early warning and the decision makers who must act on this information and yet do not have intelligence experience. There is also the problem posed by the staggering amount of information available as a result of revolutions in technology, sources and techniques. Kam suggested that perhaps this quantity of data could be better managed if analysis techniques are introduced earlier in the process at the point of data collection.

He concluded his talk by reminding the audience that while post-mortems of intelligence analysis are useful, they are not foolproof. To verify assessment procedures, analysts should aim to identify differing perspectives and issues by recognizing how the same information can lead to different assessments, and interpretation mistakes and misperceptions. Finally, Kam recommended that the intelligence community undertake a concerted effort to destroy the walls between data analysis and collection, intelligence and operations, and within intelligence organizations themselves.

Professor Dr. Karlene Roberts, Haas School of Business, University of California Berkeley

Dr. Roberts began by defining a high reliability organization as one that conducts relatively error-free operations over a long period of time and makes decisions that consistently result in high quality and reliable operations. She further clarified that "reliability" means organizational competency; more specifically, interdependence among units within organizations. These organizations should be resilient, adaptable and recognize that units are tied together and are interdependent. Accidents and errors of early warning are symptomatic of a failed trajectory of communication and information, in which units are not "making the same sense-making." Effective early warning sense-making requires trust within the organization, opening perceptual blockages to weak signals, enhancing communication and horizontal integration, and moving decisionmaking to appropriate lower levels.

Roberts then offered a closer examination of how high reliability organizations face challenges in practice by contrasting examples of where such organizations have functioned well and where they have functioned poorly. A system functions well when it engages in early model adoption, model migration and resetting (where required), integrates information and removes perceptual blockages. The system is likely to fail in a crisis when there are signals everywhere, but the individual players have no practical interdependent functions (no integration), nor practice of working interdependently. A lack of trust between units both within an organization and between organizations can exacerbate problem and result in organizational

breakdown (as in the case of the Hurricane Katrina crisis). In organizational crises, each unit has a unique view of how the crisis is changing – without appropriate integration across organizations no one will have the big picture. It is critical that high reliability organization have simple, functional organizational arrangements. Dr. Roberts highlighted the differences between a typical big city police dispatcher and responder system, which works well, and the organizational chart of Federal and State agencies charged with responding to disasters during Hurricane Katrina (see Appendix B).

Comments and Discussion

The presentations were followed by a discussion on the benefits of initiating change in intelligence organizations to overcome the hurdles facing them. Indeed, in a crisis, the problems facing high reliability organizations are not single discipline problems. As such, the variety of problems should be matched by a variety of responses. While it is more difficult to change an entire community, changes between organizations are also problematic. However, a solution is to begin to share information without initially attempting integration in order to build trust that later serves as the foundation for interoperability and interdependence. Effective forecasting and warning begin with planning and training, organizational walls can be destroyed by developing a common language.

Participants also considered the possibility that intelligence agencies may learn to share and can become learning organizations if the incentive system is changed. A team-based approach in which teams are trained, rewarded and promoted was suggested. However, the group also recognized that organizational change may be viewed by stakeholders as a challenge to professional authority and can result in opposite reactions.

Breakout Groups, Second Session (20 January 2007)

The second breakout group session offered participants the opportunity to expand on how they would address the threat scenarios presented (see Appendix A), either through practical exercises or other means. What follows is a summary of the main points raised by each group.

The Shia Ascendance in Iraq

The rise of the Shia is understood to pose a threat not just to the stability of the Middle East, but to neighboring regions as well. In response, the group advocated a multinational approach to tackling the threats posed here.

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. In line with this approach, analysts should develop a common vocabulary that can be understood by all actors working on the issue. (Another interesting, although admittedly "utopian" suggestion, was to remove politics entirely from the business and language of early warning, thus making any process apolitical and more flexible in its response.)

Access to such a system 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, something that group members agreed was needed. 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 on information and analytic systems such as these. Ideally, there should be a reward or incentive system in place for participants willing to contribute their time, effort and ideas to a common information system.

In advocating this solution, however, the group's members were keen to avoid creating new orthodoxies. Flexible thinking and working are key to addressing this and other threat scenarios.

Sustained High Oil Prices

The group examining the threat of sustained high oil and energy prices concluded that this was a foregone conclusion: high oil prices are going to be with us for a very long time to come. Consequently, rather than elaborate on intelligence or policy solutions to this issue, the group took a broader approach, one focusing on the threat posed by global warming.

Given the broad public interest in the global warming debate, the group urged breaking the problem down into smaller, more manageable problems that are easier to address: the search for alternative fuel sources, the behavior of the individual energy consumer, the instability and risks posed by oil- producing nations, and stalemate in the international policy debate. Given the range of issues currently being debated here, the best source of information is likely to be the general public rather than a single body of experts. Here then, the role of the intelligence community would be to collect, organize, analyze and synthesize the mass of data on these issues into recommendations that are actionable and sensible.

The Changing Face of Terrorism

Terrorism was defined as a complex adaptive system, one that demonstrates both subtle evolution and sudden change. In dealing with this threat, the group's members advocated improved horizon scanning exercises to try and identify where future terrorism 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 the intelligence analyst to discover new trends and understand emerging terrorist behavior in its broadest possible context. The group argued that improved understanding was also possible through qualitative rather than quantitative analysis – identifying the "who" and "why" of a given situation rather than the "how" and "when". A future horizon scanning system should be tailored to the end-customer, but should nevertheless be able to incorporate diverse expertise, social and cultural understanding, and a plurality of conceptual approaches.

The group's rapporteur added that more emphasis should be placed on strategic foresight, developing better warning methodologies, improved profiling, cognitive mapping, group cause analysis and heuristics. By improving capacities here and developing better scenario exercises, it may be possible to improve one's understanding of the conditions that lead to terrorism. In turn, it would be possible to identify preventive measures and support policy efforts to this end.

India-Pakistan

The group tasked with examining the potential for conflict between India and Pakistan began by listing possible trigger events, such as Islamist terror attacks in India and the threat of instability and regime change in Pakistan.

To anticipate and prepare for such an eventuality, the group also advocated the use of horizon scanning tools and techniques. Any horizon scanning exercise should not just consider the more traditional geopolitical tensions between India and Pakistan, but should also take note of economic, social and cultural issues, as well as media coverage of relations between the two countries. In addition, Delta scans and quantitative analysis methods may help identify future risks and triggers in Indo-Pakistan relations, while role-playing, simulated interactions and structured interviews could help improve individual understanding on how the two countries might react to one another.

The group also advocated the adoption of collaborative tools and other information-sharing systems as a means of breaking down organizational walls and improving the quality of analysis on this and other security issues.

Avian Flu Outbreak

The group examining the threat of an Avian flu outbreak argued for an adaptive intelligence system that could cope with multiple scenarios, subject areas and regional issues. This system should also be able to test different assumptions and take account of different priorities.

Given the diffuse nature of the Avian flu threat, the group's rapporteur advocated the use of software that could be accessible to a community of actors. This tool should include a timeline function so as to track the chronological progress of an Avian flu outbreak, a geographic information system or other visualization/mapping interface, and suitable collaborative tools such as blogs, wikis and electronic whiteboards to enable improved dialogue within the user/expert community. In evaluating a threat such as Avian flu, it is important to consider the potential impact of one's estimates or analyses as this could have a major (and possibly unnecessary) impact on the decisions taken by policymakers. The group stressed the importance of adopting a structured, narrative approach when examining an Avian flu outbreak, and using

the narratives of previous experiences, such as the SARS virus.

To this end, it would be necessary to bring in the opinions of different actors, including from the health and security services, the private sector and different government agencies.

Plenary and Closing Comments

The final plenary session followed the reports of the second breakout group. The purpose of this session was to consider possible pilot projects the GFF early warning community should initiate.

The session opened with comments from Ken Knight, who noted that it is necessary to experiment with new analytical methodologies and to further develop the relationship between the worlds of early warning and policymaking. Knight invited participants to suggest possible research and discussion topics on the GFF website and to detail what they hoped to get out of the early warning and foresight seminars. In addition, he stressed the idea of a pilot project, something that would be related to a real world issue and which would require the attention and efforts of more than one individual.

The seminar closed with comments from Dr. Victor Mauer, Deputy Director of the Center for Security Studies, and Dr. Warren Fishbein, Deputy Director of the Global Futures Partnership. Mauer asked the working group to think about what it could do beyond the seminar series. Fishbein ended by encouraging participants to think of ways in which to sustain this initiative and thanked them for their efforts and contributions to date.

Appendix A – Scenarios for Breakout Groups

Shia Ascendancy in Iraq

The rise of Shia to power in Iraq has created a fissure in Sunni domination of regional politics, spurred a resurgence of cultural and religious identity, and increased expectations among Shia populations who live in an arc from Lebanon to Pakistan. During the next several years, the schism between Shia and Sunni emerges as the defining regional factor. The presumption of Sunni power, the hallmark of the geopolitical system in the Middle East, is under severe threat as Shia consolidate control over most of Iraq, an emboldened Iran strives for greater power and influence, and Shia demand more political and economic attention in states such as Bahrain and Saudi Arabia.

Sustained High Oil Prices

Demand for energy continues to rise over the next two decades, particularly in the developing world. A myriad of risks to the oil market have come to pass and include: supply disruptions stemming from geopolitical hot spots such as Iraq and Nigeria and the growing strength of national oil companies (NOCs), which are unable to develop oil resources as efficiently as independent oil companies (IOCs). Moreover, natural disasters, civil strife, terrorism, strikes against oil facilities, climate change, and boundary disputes challenge the supply, production, and exploration of energy. High sustained oil prices drive the formation of new alliances, resource nationalism, and the growing strength of producers.

The Changing Face of Terrorism

Over the next 10-15 years, Al-Qaeda is weakened by the efforts of the Global War on Terror (GWOT) and recedes into oblivion. However, many of the root causes of terrorism remain. These factors, combined with the global availability of advanced technology, will drive changes in: the nature, organizational structure, methods of operation, training, financing, recruitment, targets, and means of attack. They will also affect the relationship between local, regional, and international terrorist groups.

India-Pakistan

Over the next decade, India's political, economic, and military power continues to grow. The Kashmir situation remains unresolved, terrorist attacks inside India continue, and India's relations with Pakistan deteriorate. Meanwhile Pakistan remains vulnerable to internal instability. Believing it has greater freedom due to its burgeoning position in the international realm, India appears to be mobilizing its diplomatic efforts to isolate Pakistan. This deteriorating relationship between nuclear powers poses significant regional and global challenges.

Avian Flu Outbreak

It is flu season and a new strain of Avian Flu that spreads through human to human contact appears in Thailand. Bangkok fails to rapidly identify, isolate, and contain the virus and there are early indications that it has spread to China, Indonesia, and perhaps other East Asian countries. Regional and global health organizations are uncertain as to the exact strain of the virus, the extent of its spread, and whether or not stocks of the retrovirus drug and vaccines are effective. Reports of flu-like symptoms outside Asia heighten concerns that the world is on the verge of a global pandemic. Panic ensues with potentially catastrophic implications for international travel, global trade, and economic activity.

Appendix B

Contrast between High-Reliability Organization Chart (Big City Police Dispatcher) and the Organizational chart of Federal and State Emergency Response Agencies In Effect During Hurricane Katrina
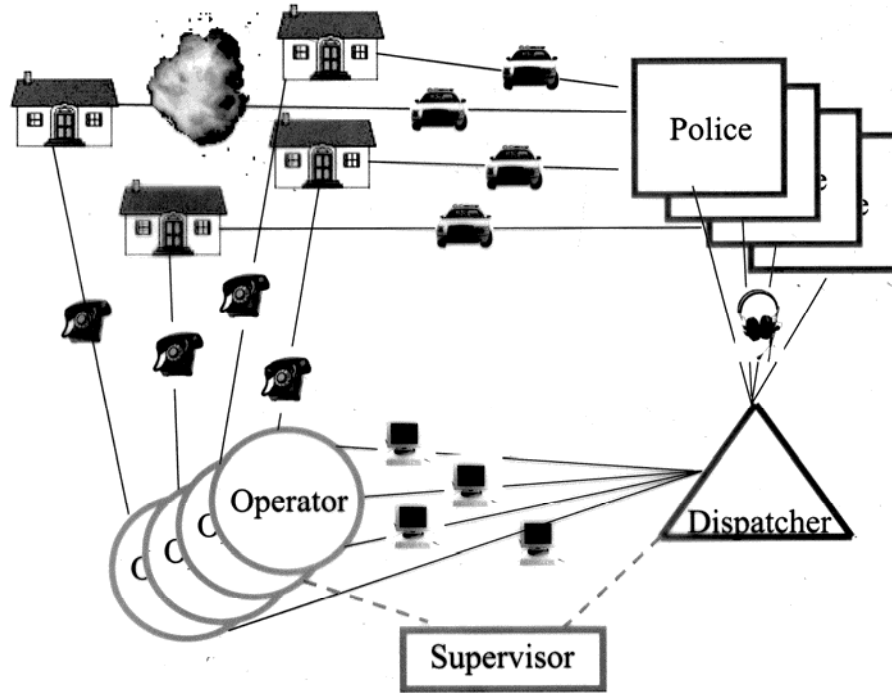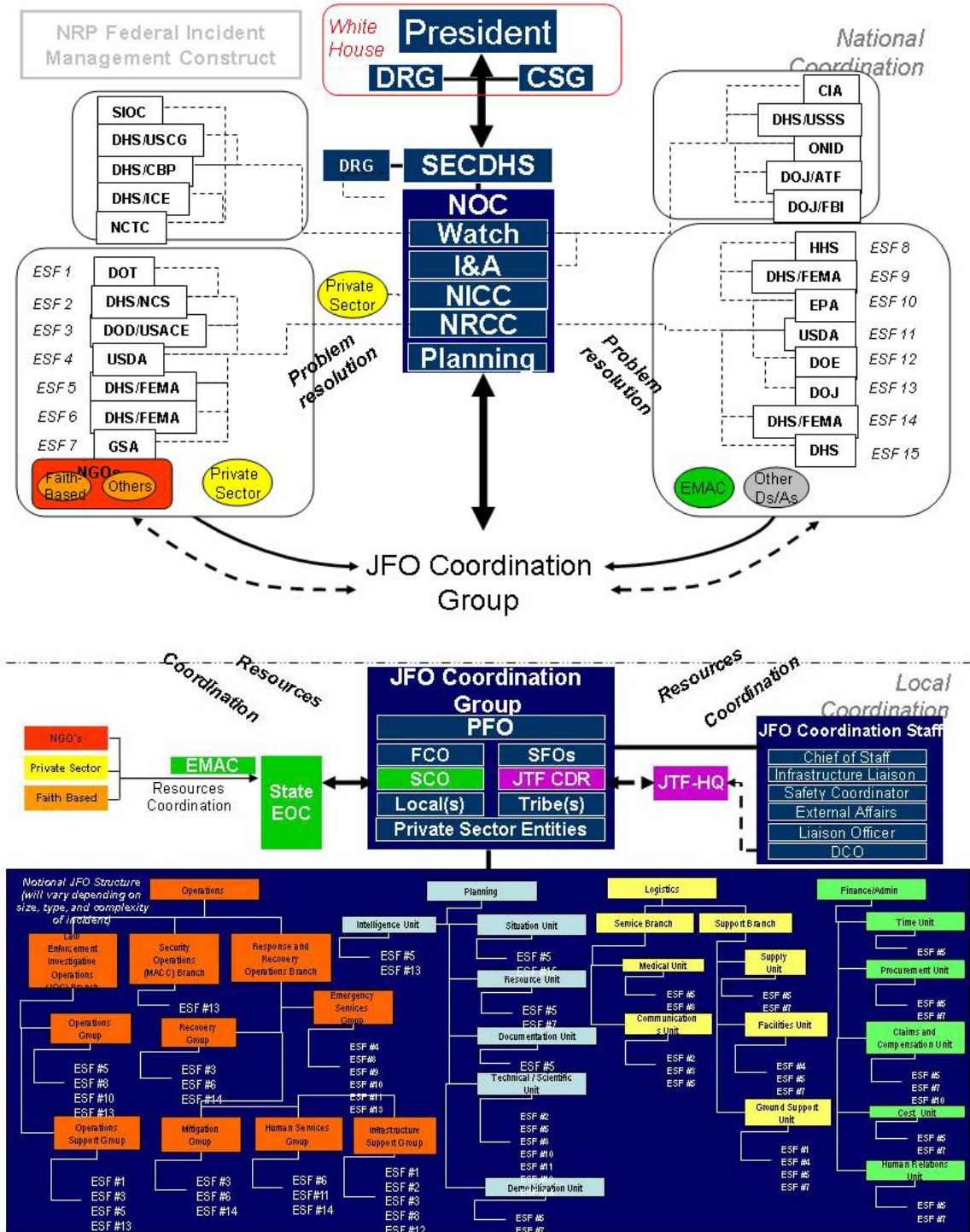

Figure 1: A large city's 911 emergency system

Figure 2: Organizational chart of Federal and State Emergency Response Agencies In Effect During Hurricane Katrina

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 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