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

Seminar 3: Warning for Readiness in the New Threat Environment

Zurich, 29-31 March 2007

CSS
An ETH Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

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

Global Futures Forum
Emerging Threats in the 21st Century

Seminar 3:
Warning for Readiness in the New Threat Environment

29-31 March 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, 30 March

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

Panel Session I: The Warning-Response Gap

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

Panel Session II: Warning for Counter-Terrorism

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

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

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

Plenary – Introduction to the Weak Signals Exercise

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

Saturday, 31 March

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

Panel Session IV: Warning and Communication: New Approaches

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

Weak Signals Exercise, Part I

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

Intelligence and Warning Roundtable

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

Weak Signals Exercise, Part II

4:00 Report Out (5 minutes each)

Plenary Discussion / Wrap Up

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

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 was 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.

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

Warning for Readiness in a Changed Environment

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

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

Overcoming the Gap Between Analysts and Policy-makers

Tensions between analysts and policy-makers are nothing new, but have gained additional attention after the 11 September 2001 attacks in the US. At intervals, policy-makers express dissatisfaction with intelligence products or even blame them for certain of their actions. They argue, for example, that the warnings are too vague and not actionable, or lead to the "cry wolf" effect and warning fatigue more generally.

Analysts, on the other hand, feel that criticism by policy-makers of intelligence performance is unwarranted and object that, even though warnings have been issued, either no action or the wrong kind of action was taken. For example, some warnings are ignored despite being actionable because they are "inconvenient", i.e., require costly or difficult adjustments or are politically difficult to manage. Others are ignored because low-tech/high-probability threats do not capture the attention of policymakers the way exotic, high-tech/low-probability threats do, despite the fact that the former should most definitely be addressed. Furthermore, if policy in general is focused too much on a specific and accepted threat, any attempt to deflate the threat is repeatedly thwarted and resources cannot be moved toward other threats that have not yet fully developed. And if policy officials have strong preferences or predispositions, they will mainly listen to analyses that confirm their preconceptions and dismiss the rest.

As valid as these points are, they should not come as a surprise. Warning is a human business and there is no simple input-output relationship between a warning given by an analyst and a foreseeable action on the policy level. Even when warnings are clear and actionable, organizational and systemic obstacles may result in diffused accountability or responsibility, or may magnify others costs and risks to such an extent that no action is taken.

Many of these grievances can be explained by lack of understanding of the other side. This is aggravated by the fact that due to the changing environment, the very nature of the "intelligence consumer" has been evolving. Now, not only top-level policymakers, but also state and local leaders, as well as the media and the public, are consumers of sorts and influence the relationship between intelligence professionals and policy-makers. As policy and policy-makers become more diffuse, it becomes harder for the intelligence community to connect with policy. Because there is no standard definition and no "typical" intelligence customer, it is necessary to improve the understanding of each others' needs. At the same time, this demands a lot of flexibility on the part of the analysts to tailor intelligence products to specific needs.

Changing Forms of Warnings

Apart from the fact that the information revolution has led to the phenomenon called "information overload" (there is too much information to absorb, due to the vast increase in open sources, and too little time to do so), more tools are available today as a result of the technological innovation. On the one hand, such tools allow for a diversity of experience, ideas, and experiments. Graphic tools, for example, could be used more widely to produce visual narratives. On the other hand, customers are now able to interact more directly with the data and thus to create more analysis on their own.

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

Furthermore, in a changing threat environment, expertise will become more valuable if it represents the complete effort of a collaborative group that can bring greater mental resources and a diversity of viewpoints to bear on a problem. Such collaborative undertakings can again be aided by new technology and can bring in policy-makers of various sorts. Examples for such networks are not only networks of other intelligence analysts working on similar issues, but can be much broader, such as high-awareness networked organizations that interlink different official actors with first-rate knowledge about the environment and situation at hand. Even though such collaboration will force a re-evaluation of traditional warning formats, it might be highly fruitful in closing the gap between analysts and policy-makers.

The Warning-Response Gap

Charles F. Parker, Assistant Professor of Government, Uppsala University, and Senior Fellow, The Swedish Institute of International Affairs

Charles F. Parker presented on lessons learned from the warning response problem in the cases of the September 11 attacks and Hurricane Katrina. He began by defining a surprise as an "abrupt revelation that one has been working with a faulty threat perception regarding an acute danger." The main elements inherent to a surprise are: the event is contrary to the victim's expectation; there is a failure of advance warning; and the event lays bare the lack of adequate preparation.

Most "surprises" happen due to a failure to act (not a failure to see). In the case of September 11 or Hurricane Katrina, for instance, a variety of past experiences with terrorist bombings and hurricanes could have been regarded as indicators of what might happen. The key question therefore is why do governments fail to adapt to a changed environment?

Parker identified different categories of obstacles to sufficient vigilance: psychological factors; bureaucratic-organizational factors; agenda-political factors; and problems of disorganization, denial and distraction.

- First, several psychological pathologies play an important role: overvaluation of past success, overconfidence in current policy, insensitivity to warnings critical of existing policy and threat warnings, wishful thinking, cognitive overload and interpretive ambiguity (signal-to-noise problem), and receptivity fatigue (the "cry wolf" syndrome).
- Second, organizational aspects also contribute to diminished vigilance: organizational fragmentation, a lack of cooperation and insufficient coordination, bureaucratic conflict, as well as neglected standard operating procedures (SOP).
- Third, agenda-political factors provide further reasons: overcrowded agendas and competing political priorities distract decision-makers from providing leadership in terms of setting the right priorities. Other interfering factors are framing failures in terms of not placing issues high enough on the political agenda.

Parker criticized the excessive focus on terrorism has inhibited the intelligence community's ability to concentrate on much more frequent threats. He also acknowledged there are grounds for pessimism concerning possible reforms to eliminate surprises. The potential for danger lies, for instance, in the creation of new problems as a result of hasty reforms, over-learning and over-reactions, the "fighting the last war"-syndrome, as well as the enduring nature of the previously-mentioned psychological, organizational and political pathologies.

There is, however, reason for optimism as well: the problem of eliminating surprises has received increased policy attention and increased funding, thus, government capabilities and interagency cooperation are both improved. No magic formula exists for coping with the warning-response problem, but progress on organization, process management (for example, institutionalized systems for keeping lessons learned) and leadership (such as career incentive alignment) is possible.

Jim Wirtz, Professor in the Department of National Security Affairs, Naval Postgraduate School, Monterey

Jim Wirtz started by pointing to four critical aspects of an "indicator and warning" (I&W) system: information suggesting capability and intentions of undesirable activity are increasing, information suggesting the ability to obtain signals is diminishing, missing data and the risk assessment problem.

The key issue in risk assessment is to determine a credible, proportionate response for each step of the general alert system focused on the overall threat. It is crucial that appropriate protocols for addressing issues at each step are established.

The classical I&W view is directed at known threats and based on well-known indicators. In the contemporary setting, however, this has changed. For Wirtz, the history of intelligence failures is a history of information not recognized. The problem is neither a lack of information, nor a lack of imagination. It was already clear before September 11 that terrorists were interested in the World Trade Center because it had already been attacked.

The real problems are rather the rationality bias on the part of analysts and policymakers and the gap between the costs of a response, which are known and real, versus the theoretical costs of attack. In addition, the "all or nothing" response to warning by policymakers further aggravates the problem, meaning that if it is not possible to solve the problem, they are not at all interested in dealing with it.

A number of external and internal challenges to warning can be recognized. On the external side, the challenge sums up to the question "what is the threat?" In contrast to what is often said about the threat picture after the Cold War, the current threats are generally known, according to Wirtz, and signals are generally available. However, some other important questions need to be addressed: For instance, what is irrational? What is rational?

Concerning internal challenges, I & W processes are all directed to where we are failing, but why do we not focus equally on our successes? The rationality bias, a lack of cultural awareness, or the expectations of specific and accurate warnings on part of policymakers further represent challenges for the warning community.

Wirtz recommended detecting anomalies by observing the presence or the absence of certain factors. He also suggested paying attention to standard operating procedures (SOP): even small changes in SOP can derail threats, overcome the rationality bias and overcome the response bias. If only small changes had been made in airplane security prior to the September 11 attacks, it might have been able to prevent them.

Discussion

The discussion centered on the recommended changes in SOP. Wirtz reaffirmed that we all have our patterns, following routines and acting very similar from day-to-day. This is an observable for everyone, also for potential terrorists. Changing SOP's and bringing irregularities into our patterns of behavior might be an effective response. It is also a low-cost policy option, making it appealing to policymakers. However, some participants stated that while it might be low-cost to the government, it may impose high costs on individuals, as the restrictions on bringing liquids on board of airplanes clearly illustrates.

Warning for Counter-terrorism

John Sullivan, LA Sheriff's Department, Terrorism Early Warning Group

John Sullivan opened the panel session with a presentation on the subject of distributed early warning, high awareness networked organizations and the co-production of intelligence. He began by examining in detail how changes in the global threat environment have been experienced on the ground by local law enforcement and emergency management organizations. In particular, he explained how the new threat environment has been marked by the tendency of local operational spaces and threat actors, to evolve into more globalized phenomena. Mr. Sullivan went on to discuss the challenges posed by global cities (metropoles), lawless zones that–challenge the rules of governance, failed states, as well as ungovernable communities and even buildings. He also spoke about the impact of networked diaspora communities and virtual groups that extend the area of concern beyond the traditional realm of normal policing. Sullivan highlighted the importance of examining a local threat with the aim of understanding the global influences that shape it. For instance, US deportations of LA gang members have now given the groups a global reach.

Sullivan further considered the challenges of adapting the traditional national security outlook. Global threats, he noted, require global responses. In the case of the United States, a lateral cooperation level seems to work on the federal level thanks to long-standing US institutional traditions. However, the centralization of diplomatic cooperation is much harder to achieve on the level of the Executive branch.

Ensuring lateral cooperation has required significant internal reform on the part of law enforcement and emergency agencies, none of which can weigh public safety against the interests of national security. Because of the linkages between the local and the national, and between the national and the global, security agencies at all levels have to be better synchronized.

One example of this can be seen in Los Angeles. The LA riots led to a citywide response that evolved into the Terrorism Early Warning network. Relying on the support of outside consultants from RAND, LA sought to create a network of terrorism liaison officers and infrastructure liaison officers. The goal here was to create intelligence fusion centers that would assess threats pre-, trans- and post-event. By doing so, they hoped to move away from the traditional perspectives on national security and law enforcement, which has maintained a rigid separation of mandate as well as areas of responsibility and capabilities. The overarching mission statement of the terrorism early warning network is to develop operational intelligence and contribute to the co-production of intelligence across terrorism early warning and the intelligence fusion community in order to prevent, counter and respond to terrorism and emerging threats by conducting indicators and warning (I&W) and operational net assessment.

This network is comprised of specialized assessment units that focus on consequence management, epidemiological intelligence, forensic intelligence and investigative liaison. At the heart of this activity is the analysis/synthesis cell, which receives and distributes reporting from all related specialized assessment units. Coordination is facilitated by the standardization of the network processes that function in a four-step operation: inputs (such as tasks, leads and reports); process (collection managements, prioritization, process, product/analysis); output (tailored products, assessments and synchronization); and outcome (actionable intelligence and its dissemination).

Sullivan concluded with a discussion of intelligence preparations for operations, deep indications and warning, the transaction analysis model and cycle, and a review of some of the lessons learned in the early warning network building process. In particular, he reminded participants to vet and validate inputs, irrespective of the source, including intelligence from federal sources.

Longer-Term Foresight in the Policy Process

Alexander Van De Putte, Professor of Strategic Foresight, Geneva School of Diplomacy and International Relations

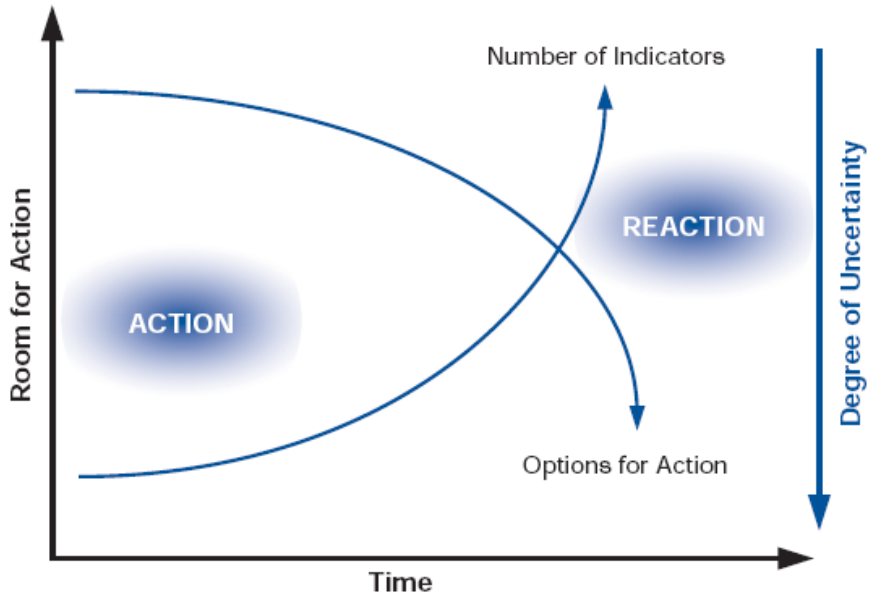
Alexander Van De Putte began his presentation by noting that when he talks about long-term foresight he means a period of 10 or more years. Within this time frame discontinuities and unexpected events are likely to occur. Extrapolating the future from current trends is not always a sensible exercise.

Van De Putte introduced three strands of scenario planning: the Anglo-American school; the "La Prospective" school, and the Probabilistic Modified Trends school, which also has two branches – trends impact analysis (TIA) and cross-impact analysis (CIA).

The "La Prospective" school, whose major theorists include Michel Godet, is the preferred approach for Dr. Van De Putte and is used for strategy setting, policymaking and longer-term foresight. In essence, this approach is a blend of the other two schools. It is intuitive and narrative but also has quantitative elements.

Using this school, he mapped 23 core global risks sub-divided into societal, economic, geopolitical, technological and environmental groupings. Societal risks analyzed included pandemics, infectious diseases and liability regimes. Economic risks included the oil price shocks, fiscal crises caused by demographic shifts and a Chinese economic hard landing. Among the geopolitical risks identified were international terrorism, the proliferation of weapons of mass destruction, a retrenchment from globalization and the continued instability of the Middle East. Technological risks included the breakdown of critical information infrastructure and the emergence of risks associated with nanotechnologies. In addition, environmental risks that ranged from climate change to natural catastrophes were also included.

According to Van De Putte, the number of risks we face is growing steadily. This creates a policy dilemma: as time passes our ability to respond effectively to these risks is greatly reduced. Typically, our response to risks shifts from prevention to adaptation. Invariably, the policy of adaptation is more costly than that of prevention.



There are five pathways to mitigating this problem: 1) improving insight on how risks may develop over time; 2) enhance the information flow on these risks so as to improve knowledge; 3) refocus incentives to action; 4) improve investments to find solutions; and 5) implement solutions through institutions.

Van De Putte noted that good foresight tools need to be inspirational and tangible and need to appeal to both the heart and mind. Most challenges cannot be addressed by anyone acting alone. Thus, concerted effort is necessary across a range of actors and institutions. Finally, participants were reminded that a policy of prevention is always better (and cheaper) than a policy of adaptation.

Craig Gralley, Director, Strategic Plans and Outreach, US National Intelligence Council

Craig Gralley's comments were based on an earlier project for the US National Intelligence Council (NIC) that led to the publication, *Mapping the Global Future*. This project brought together over 1,000 participants at five global conferences. It sought to examine "wild card" threats and opportunities, as well as upcoming trends.

The "Mapping the Global Future" project sought to mesh long-term foresight with the policy process and explore global trends to 2020. It examined globalization as a megatrend, explored the emergence of China and India as global players, considered the evolution of the terrorist threat, and analyzed the likelihood of great-power conflict.

The ultimate goal of the project was to stimulate debate. However, the report itself was not widely read in policy circles.. In addition, its message was also misinterpreted: described in the zero-sum terms of "rise and fall." However, its reach and impact was both domestic and international. The report was picked up by think tanks in US and overseas, where the response was greater than expected. Although the report did not have a big splash on the US policy community, its ripples were felt beyond the more obvious quarters. Its biggest impact was on the NIC itself, which adjusted its perspective and agenda as a result of its findings.

The NIC's next project is an effort to map the globe in 2025 and will begin later this year with a final report due in late 2008. It is hoped that the incoming administration will be receptive to the reports findings. Again, international conferences will be organized to look at traditional and non-traditional issues before a final report is written.

Martin Briens, Directeur Adjoint du Centre d'Analyse et de Prévision, Ministère des Affaires Etrangères, France

Martin Briens began by asking whether long-term foresight was of any practical utility to policymakers. The key difference between those who provide foresight and policymakers, he reminded, is accountability. Twenty years from now, few will remember the estimates and assumptions of foresight experts, whereas the decisions of policymakers could have very real long-term consequences.

Briens went on to note that it's difficult to integrate foresight into the policy process. That said, the process isn't impossible either. For instance, urban planning, the interplay between demographics and economics, is one example where long-term planning enjoys a successful relationship with policymakers. The same can also be accomplished in realm of the defense and intelligence.

The question remains, however: why worry about the future when the past has enough challenges of its own? Policymakers have to deal with one crisis after another and there is little room for strategic thinking. A report on China in 2030 may make for interesting reading, but of what relevance is it to today's policymakers and the challenges they face?

Briens warned that for long-term planning to be more relevant, it has to avoid Western biases. People tend to ignore long-term historic trends: not everything is the product of Euro-Atlantic activity. Thus, a closer reading of history and improved understanding of global opinions are both essential.

He went on to argue that most policymakers move forward with either "eyes wide shut" or a political sixth sense. Indeed, their response to future risks falls into one of three modes: 1) ignore it; 2) prepare for it through adequate insurance planning; and 3) help actively shape it. The last response is the most daring and the most responsible, but also the least common.

What can be done, therefore, to better integrate foresight into the policy process? Briens argued it is important to give policymakers a sense of ownership in whatever issue they are asked to address. Second, it is essential that intelligence analysts clearly present and clarify the possible policy choices and their implications. And finally, he emphasized the importance of having the right decision-making processes in place.

Discussion

In the discussion that followed, the chair, Martin Ortega, a senior fellow at the EU Institute for Security Studies in Paris, noted the growing importance of future studies both as an academic and political discipline.

One of the participants asked whether intelligence agencies made a habit of reviewing their previous estimates to see what they got right and what they got wrong. It was generally agreed that a history of foresight would be invaluable in helping to understand the challenges and dilemmas inherent in the foresight business.

It was also noted that time horizons are shrinking and that this necessitates a new methodological approach to foresight, one that is more aware of the speed of change and the complex array of forces shaping the world and the work of intelligence. Scenarios now have to be reviewed every three years in order to test their validity against prevailing conditions.

Further to this, one participant noted that scenario exercises are not prediction exercises. One can create multiple scenarios but there will only ever be one future.

Finally, another participant noted that in the business of foresight, analysts risk projecting their preferences and biases on a people they may never meet. It's worth bearing in mind that we may well be living someone's "nightmare scenario".

Warning and Communication: New Approaches

Henry Farrell, Assistant Professor, Department of Political Science, George Washington University

During the third panel session on new approaches to early warning and communication, Henry Farrell addressed the relevance of blogs and early warning. He began by evaluating what is known about blogs as a modern communications phenomenon – from their early appearance as an internet oddity, to their subsequent adaptation as a communications platform, and finally, to their emergence as a widely used media format with national and even international resonance. He also discussed some of the more significant growth trends of the blog, in particular its rapid spread in Asia, and signs that the market is beginning to saturate (there are currently between 45 and 75 million blogs according to some estimates).

Farrell then shifted his discussion to consider the broader impact of blogs. Blogs represent a vast set of distributed conversations (some across national boundaries) and can substitute for media and conversations that don't exist anywhere else. These conversations can be and have been mapped. Research reveals that blogs are often cross-national bridges; some are more important than others and some serve as gatekeepers on a given discussion topic. Within these discussions there are key blogs focusing on particular topics; and within these topics there are key voices on given issues. All can have an impact, whether indirectly by shaping the discourse, or more directly by giving rise to reactions and responses with direct consequences.

Because of their fundamentally accessible nature (due to the ease and low-cost of set-up and operation), bloggers can act or respond to an event within hours. This has had the effect of speeding up the rate at which controversies are brought to the fore of public debate and onto national agendas. As such, blogs can serve as early warning indicators for change. They also have the potential to serve as substitutes for media and political debate in the public sphere.

However, their relevance to intelligence analysis, while significant, is also limited. This stems from the problem of weak signal-to-noise ratio, which is very real in this medium. While blogs do play an important role in disseminating ideas, arguments and information, it is extremely important for intelligence analysts to actively distinguish information from noise when searching for weak signals in blogging communities.

Analysts must factor elements such as bloggers' intentions and their intended audience, all of whom are invited to shape the content further. One should also take into consideration the fact the bloggers rarely represent the general population and that those living in non-democratic countries will broach their subjects in a very indirect way.

Farrell further cautioned that while blogs will not reveal terrorist plots or plans, they will reveal how terrorists communicate, recruit and use technology. Blogs that fulfill an analyst's preconceived notions should never be the focus of analysis, as these blogs reinforce analyst bias.

Michael Schrage, Co-Director of the MIT Media Lab's e-Markets Initiative, Senior Advisor to MIT's Security Studies Program:

The second speaker addressed the topic of new approaches to warning and communication from the perspective of adapting tactical innovations for strategic warning. Drawing on comments from the intelligence community, he began his discussion with an examination of innovation in organizations.

Innovation is not always what is created, but can also be manifest in what is adopted. Mr. Schrage also noted the usefulness of examining the artifacts of innovation and other experiments to better manage the process of innovation.

From this, Schrage proposed a reframing of traditional warning definitions to the innovative view that warning is an "invitation to the recipient to act". From this perspective, a warning also has implications for the analyst, such as distinguishing between public (open) vs. private (secret) invitations, and to whom these invitations should be extended. Schrage cautioned that warning could become an instrument of information warfare. The analyst community should consider this aspect much more explicitly when framing its reports.

Schrage then drew his remarks to customers of warning, noting that one of the consequences of technological innovation is that more tools are available to everyone, including policymakers. On the one hand, such tools allow for a diversity of experience, ideas and experiments to interact. On the other hand, it has given rise to the phenomena Schrage dubbed as "BYOA = Be Your Own Analyst." Customers want to be able to do more of the analysis on their own, that is, to interact more with the data.

Rather than resist the trend, he suggested the intelligence community consider creating models, tools or simulations that invite iterative interaction by intelligence customers, thus allowing policymakers to have greater interaction with intelligence data. This would provide several advantages; in particular, it would allow policymakers and other customers to persuade themselves of the integrity and accountability of the intelligence products they receive. This would necessitate a profound, epistemic "design shift" from "best possible facts that productively informs" to "best possible facts that productively invites."

Carmen Medina, Director, Center for the Study of Intelligence, Central Intelligence Agency

The third speaker, Carmen Medina took a broader approach to the subject of warning and communication and focused on how changes in the new security environment will change the work of analysis. She began with an examination of the needs and expectations of analysts and policymakers and urged the participants to consider a more narrative-based approach to warning and to move away from the traditional prose-oriented reports to narratives that tell a story. This would have the effect of making warning more relevant and clear to the ultimate recipient – policymakers – few of whom are masters of the obvious.

Medina offered five trends that are shaping intelligence analysis and warning.

- First, the technological shift from analog to digital analysis. The technology that has given rise to innovations that enhance the collection of intelligence have also resulted in a much greater rate of information creation. These factors will change what analysis is.
- Second, Medina anticipated graphic tools will be used more widely as visual narratives and the dynamic spectrum for analysis will move from the forensic to the conceptual.
- Third, the traditional model of the individual analyst at the center of the intelligence process is receding. Expertise will matter more in terms of how it describes the complete expertise of a collaborative group. Expertise in collaboration will become more important. Medina argued that there would also be increased demand for collaborative communities of analysts that can bring greater mental resources to bear on a problem.
- Fourth, the role of the analyst is also evolving to that of the hybrid analysts: every analyst will become a collector of intelligence and vice versa. Over time, the role of the analyst and collector will blur and become one.

- Fifth, the intelligence community will experience a wider adoption of collaborative platforms (such as wikis) to do the work of analysis. These platforms will force a re-evaluation of traditional warning formats. Medina argues that these platforms can provide important opportunities to harvest the weak signals generated in the background of analysts' debates.

Discussion

In the discussion that followed, participants considered some of the challenges of providing warning, including how to determine whether policymakers have been adequately warned, and the differences between strategic warning and tactical warning.

One participant cautioned that while warning is an invitation to act, senior policymakers don't want a scenario in which they are being warned about something for which they personally will be held accountable. The message must be delivered in a more effective manner. A participant suggested warning should also be offered to prepare top-level politicians for events, as a kind of expectations management tool.

The discussion shifted to the subject of blogs and how they are affecting closed societies and their governments. Farrell noted that while there is a relationship, it is difficult to find any hard, causal evidence between online conversations and government actions. Although there is some evidence of impact, the reality is that in super-closed societies such as North Korea, it is difficult for most people to access and use this technology. In the case of Iran, blogs flourished after government crackdowns on magazines. The impact of blogs can also be seen in China, where government officials continue to censor particular websites and individuals.

How governments will be affected by blogs seems primarily indirect; that is, blogs will create a kind of civil society outside of the control of the state. This can have both positive and negative consequences. However, the expectation is that the indirect effects will be greater than the direct effects.

Finally, the discussion moved to the issue of managing data sources in the new environment. While the scale of information has grown, there remains a large amount of data that isn't data as such (spam, old information and old programs). Nonetheless, all this information will require greater collaboration within the intelligence community. The challenge remains in turning quantitative data into relevant qualitative data – if one has data one must understand it. A quantitative analysis is only as good as the hypothesis that generates it.

Breakout Groups

The breakout groups were given a twofold task: on the one hand, they were asked to reflect on the Fountain Park exercise, which participants had undertaken prior to the conference; on the other hand, they were tasked to discuss the lessons learned from the seminar in a broader context.

Specifically, the following four questions served as guidelines for discussion in the five breakout groups:

1) What is the relevance of weak signals for policymakers?
2) How can the Fountain Park tool and other approaches help in putting weak signals on the radar of policymakers?
3) What are the most important lessons learned with respect to providing early warning to policymakers and operations?
4) How does the discussion in the breakout group challenge our understanding of the process of early warning?

The first group emphasized three major points: First, the need for customer-focus. The customer base is much larger than it used to be with more stakeholders wishing to get informed and to be involved. It is increasingly necessary to apply a top-down as well as a bottom-up approach. Second, one single tool is not sufficient anymore. What is needed is a portfolio of tools, adapted to the different needs and demands of the broadened customer base. Third, warning must be understood as a constantly ongoing, interactive process.

The second group affirmed the need for more interactive ways of working together. They pointed to the ambiguity of consequences and fundamentally challenged the warning community by asking whether the notion of warning as such is still relevant today.

The third group reiterated the necessity of a portfolio of tools and stressed the importance of skillfully managing expectations of decision-makers. With regard to the relation between experts and decision-makers they said that the latter draw on many sources of information as well as their own "vision of the world". For the analyst it is therefore crucial to have the right timing, to develop a sense of urgency, to employ different channels, or to understand the personality of specific decision-makers in order to be able to influence and convince them.

The fourth group emphasized the relevance of weak signals because they may indeed indicate emerging trends. They also concluded that many of the restraints imposed by formal procedures impede effective warning. Further, the need of a history of foresight was raised. Finally, the group asked provocatively whether the warning community is learning at all, or whether it the same questions are asked time and again without getting any better.

The fifth group wondered whether the weak signals identified by the Fountain Park tool were really weak signals or just outliers from consensus view. Nevertheless, the tool stimulates debate because it facilitates a "devil's advocate" approach. In terms of improving relations between analysts and policymakers, the group suggested better coordination and more intense cooperation. Intelligence is only one input among many that decision-makers receive and the warning community must improve its capability for effectively conveying its message to them.

Intelligence and Warning Roundtable

Introductory Remarks by Alyson Bailes, Director, Stockholm International Peace Research Institute (SIPRI)

The roundtable began with comments from Alyson Bailes on the nature of warning and its role in the policy process. Bailes asked whether warning was part of a circular process or something more interactive, especially given the tendency of policymakers to take on the role of analyst. Clearly, warning is no longer a simple, linear process.

Bailes noted that in any event, the quality of the warning had to be matched by a quality of attention on the part of the policymaker. She reminded the audience that warning is an invitation to act: both steps have to be matched by a quality of response.

Jorge Dezcallar, Secretary General, International Advisory Board Repsol-YPF and Former Head of Spanish CNI

Jorge Dezcallar opened his comments by warning that we are not well equipped to confront the current range of threats. Today's terrorists seek to benefit from the forces of globalization by identifying "soft targets" and creating havoc in our societies. Our defenses against such attacks are inadequate. As such, we have to accept that we are vulnerable. In reducing this vulnerability and in confronting terrorism, we must never compromise our liberties or the values we hold dear.

Dezcallar argued that being honest with the general public and acknowledging the vulnerability of our societies is actually one of the most effective means of dealing with the risk. People react well to honesty: They know what's at risk and what role they have to play in ensuring their own safety.

He went on to note that information was the greatest impediment to effective early warning. All information sources have their limitations. Before the Madrid train bombings of March 2004, there were a number of sources warning of an attack, none of which expected an attack in the heart of Madrid. Much of the information being collected was vague and unclear; this limited the ability of the Spanish security services to act effectively.

Intelligence personnel, noted Dezcallar, don't always have the full picture. As a result, they are wary of damaging their credibility by acting too soon on incomplete information. Unless they have good contacts in other agencies or departments, the level of information-sharing is always constrained by institutional and organizational regulations and culture. An analyst with only a partial picture of what's going on is unlikely to act without further clarification – which in itself may never be forthcoming.

Similarly, before beginning any surveillance operation, intelligence personnel need to obtain permission from the relevant judicial authorities. However, these authorities are unlikely to grant permission for such an operation without also being given a full, unambiguous picture of the situation at hand and why it poses a threat. If the picture isn't clear, permission won't be forthcoming.

Dezcallar concluded by reminding the participants of the cautionary tale of the boy who cried wolf. In this instance, the warnings were not without merit, but absent sufficient information, these warnings were not taken seriously enough. Ultimately, one cannot make people afraid without good reason and sufficient evidence.

Reid Morden, former Deputy Foreign Minister and former Director of the Canadian Security Intelligence Service, and President of Reid Morden & Associates

Reid Morden's comments were based on his professional experience as a producer and consumer of intelligence. He noted that the rising dangers in the world require better analysis from an increasingly complex range of disciplines. Analysis is always a difficult business, especially, when the personal biases and emotions of the consumer inevitably intrude. Moreover, governments are always driven by what's urgent rather than what's important. In such an environment, it is important to avoid "warning fatigue".

This history of warning, he reminded the audience, is not an illustrious one. No one predicted the arrival or the consequences of the Bolshevik Revolution, the Great Depression or the Cold War. The discontinuities of yesterday still affect the intelligence processes of today. What the intelligence community has to understand, he cautioned, is that the urgent will always come first.

Therefore, the number one task of intelligence providers is to persuade the consumers of a real sense of danger in a credible way. The ease or difficulty of such a task largely depends on how much policymakers are used to using intelligence for decision-making. Moreover, intelligence providers have to temper the dangers they confront with pragmatism. The crystal ball will not always yield the information necessary to make a decision. Analysts must avoid overstatement lest this detract from the credibility of the provider and thus limit the ability of the policymaker to recognize the problem at hand.

In contrast, the policymakers themselves have to take warning seriously. Often, local governments are mesmerized when receiving intelligence from the national government and fail to connect it to their immediate circumstances. Conversely, national governments often do not appreciate the importance of filtering up from local authorities. More often than not, critical intelligence is locked in a safe by security professionals where it remains inaccessible to those who have to implement policy. Morden also noted that knowledge-sharing is not a natural inclination of the security professional and highlighted the importance of packaging intelligence so that it can be more easily digested by its intended audience. The providers of intelligence have to think more carefully about what they produce. Do they wish simply to plant the seeds of warning, and or educate the consumer and/or encourage them to act. Thus, foresight should always be, to quote Alex van de Putte, "tangible and inspirational".

The speaker repeatedly stressed the dangers of warning fatigue. A telling example of this is the bombing of Air India 182. The Canadian civil aviation authorities refused to order additional resources to screen baggage despite repeated warnings of an attack.

Policymakers will not necessarily shy away from difficult issues but intelligence providers must meet policymakers' needs for material persuasive not only to themselves but also to their peers and superiors. Analysts must therefore help policymakers to identify the risks, delineate the impact if something should happen, connect the future to their interests and prepare accordingly.

Barry Pavel, Interim US Principal Deputy Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and Interdependent Capabilities

Barry Pavel began by noting that as a user of intelligence products, he found that most of these products were very good. During the 1990s, he worked on the enlargement of the NATO alliance. As part of this process he performed policy planning analysis in order to understand what impact the enlargement process would have on the US, the former Soviet-bloc states and on Russia.

Pavel noted two challenges for the intelligence community: a) a tendency to answering the wrong questions and b) answering unasked questions. To address these challenges he offered six recommendations. First, broaden the aperture of intelligence analysis, especially in terms of time, space and scope. Second, imagine the unlikely. It's essential for analysts to present policymakers with possible long-term scenarios. Pavel encouraged analysts to "go long" and bring the future into the present. As part of this process, analysts must work with policymakers to answer unconventional or unasked questions. Third, it is essential for intelligence analysts to interact with the policymakers and understand their policy objectives. The boundaries of the intelligence/policy nexus have to be reconsidered and redefined as part of an ongoing, iterative process. Those lines that could hitherto not be crossed must now be re-examined in light of a changing threat environment.

Fourth, it is essential that the intelligence community be clear on the where and why of its mistakes and successes in the past. Moreover, it must understand what impact its successes and failures have had on its current assessments. A closer assessment of past performance is essential. No one would invest in mutual funds without some indication of past performance. Thus, no one will invest in an analyst's recommendations without prior information.

Fifth, more thought needs to be given on what it means to be an intelligence professional. What are the new metrics of measuring success or failure? What new skills are needed to perform effectively? Professional intelligence standards need to be reevaluated. Finally, there must be greater emphasis on the importance of integration across different departments, security agencies and national boundaries.

Pavel also noted that one of the biggest challenges facing the intelligence community is a lack of imagination. There tends to be a paucity of imagination that necessitates a broader aperture in terms of intelligence forecasting. By broadening their perspective, analysts can keep policymakers better informed as indicators develop and change. They can also recommend low-cost hedging strategies against possible threats long before they become really pressing.

Ken Knight, US National Intelligence Officer for Warning

--

Discussion

The discussion that followed allowed the audience to respond to the statements of the panelists. One participant noted a concern that intelligence agencies were condemned to respond to risks and challenges and were not suitably prepared to exploit opportunities. It isn't always clear if capitalizing on opportunities is part of an intelligence agencies remit.

Another participant commented on the difficulties of broadening the imagination of intelligence analysts, especially with regard to risks and threats. The most imaginative people are often the most difficult to work with. Integrating their ideas into the intelligence process is always a challenge. In response, the panel noted that the solution lies not in fixing the analyst but in fixing the organization, or even the policymaker. Imagination cannot be stifled simply because of having to manage character defects. Intelligence agencies should use different tools and fora to mix things up and get new ideas flowing. Bringing in outside experts could be one way of encouraging new ideas and fostering imaginative solutions.

Another participant warned of the danger of engaging too closely with the policymaking process. The risk here is that the intelligence analyst also becomes an advocate for the policy, even though that's not their job. The risk here is that policymakers can "use" intelligence analysts to justify their actions. This is a risk that is best avoided.

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