New Frontiers in Intelligence

Notes from seminar in Stockholm May 27-28 2008

Center for Asymmetric Threat Studies (CATS)

Editor Gregory F. Treverton

CATS
Center for Asymmetric Threat Studies

SWEDISH EMERGENCY MANAGEMENT AGENCY

Title: New Frontiers in Intelligence, Notes from seminar in Stockholm May 27-28 2008
Editor: Gregory F. Treverton

Published by: The Swedish National Defence College
Number of copies: 400

ISBN 978-91-85401-99-4

Printed by Elanders, Vällingby 2008

Center for Asymmetric Threat Studies
New Frontiers in Intelligence

May 27-28, 2008
Gregory F. Treverton

Headlines:

- The distinctions on which Cold War intelligence was based – intelligence-policy, analyst-collector, internal-external, intelligence-law enforcement – no longer apply.
- As Stevan Dedijer noted long before others, all organizations require intelligence if they are to survive. As Madonna might put it: "We live in an intelligence world."
- The sources of error in NGO "intelligence" ran intriguingly parallel to those of government – stereotypes (Afghan resistance from "freedom fighters" to "terrorists"); unilateral sources; false categories; distortions across cultures; unquestioned assumptions and unverified information; prejudice and mind-sets; projections; groupthink; too much power to precedents; simple information overload; disinformation; and the pursuit of false consistency.
- For organized crime, intelligence is not a specialized role; everyone keeps his eyes open. The focus is tactical and low level. What is gathered has to make a difference pretty soon. Collectors and analysts and users are all the same.
- The shift to transnational threats is the transition from a small world with large threats, like nuclear war, to a large world with small, hard to identify threats and the absence of stable ideological coalitions that instead lead to asymmetric campaigns.

- Much of what passes for "strategic analysis in law enforcement is too general to be helpful – "the price of heroin is falling in Russia," for instance. Instead, what is needed is a process to establish some priorities, by working both from the top down using strategic areas, both regional and functional (Balkans, eastern Europe, human smuggling, cocaine, criminal organizations (prison or motorcycle gangs, for instance), and from the bottom up through known or suspected criminality among groups or individuals.
- Dogs that didn't bark – warnings of events that didn't happen – resulted from warnings producing action, mirror-imaging, wishful thinking, predicting convenience, missing variables and the self-interest of the warners.

****

The goal of this workshop, the first in the second year of work on intelligence for transnational threats, like terrorism and homeland security, sponsored by the Swedish Emergency Management Agency (SEMA) was to look in depth at two key frontiers for intelligence in an era of terror: 1) To understand and learn lessons from new and non-traditional fields of intelligence and new actors, from non-governmental organizations (NGOs) to organized crime; and 2) To address intelligence "complexities" – that is, issues or threats, like that of terrorism, that may involve large numbers of relatively small actors responding to situational factors that do not necessarily repeat established patterns.

Setting the Scene: The changes in the context of intelligence since the end of the Cold War are by now familiar, but their force remains hard to calibrate. Surely, the threat from the jihadis is more complicated, for they are networked and make use of technology in surprising and sometimes innovative ways. The distinctions on which Cold War intelligence was based no longer apply in the way they once did:

- Intelligence-policy "membrane." Even with the Cold War's separation and shunning by intelligence of contact with policy, there was some influence. Now, it is necessary to integrate interests in an interactive project between intelligence and policy.
- Analyst-collector "wall." This too is and has to be much more permeable than it was when collectors mostly passed data "over the wall" to analysts. Today, it is crucial to bring analysts and collectors much closer together (virtually and/or physically, organizationally). To be sure, there are security risks involved in this, but they are outweighed by the potential gains of this close cooperation.
- Internal-external "wedge." Traditionally, cooperation between internal and external intelligence services has not been good; often the "other" service

is seen as an interloper or a party pooper. Yet reality is breaking down this wedge as well, and with it, the concept of "need to know" is also changing. Various organizational set-ups have been tried to address this wedge, but only very few have proven to work satisfactorily. In one country, the internal service is being transferred from Justice to Defense and it will be interesting to see what difference that will make.

- Intelligence-law enforcement "divide." Here, too, where one ends and the other begins is becoming blurry in ways with which national decision-makers, lawmakers and judiciaries, as well as our publics have not yet come to grips.

Overcoming these distinctions is not necessarily a new challenge, but it is imperative now. It means both "doing the right things" and "doing things right." In the first category are finding niches, operating with less secrecy (unless absolutely necessary), getting closer to consumers and at the same time knowing when to say "no" to political masters, and knowing where to find information outside intelligence and outside government but recognizing that the process has to be a two-way street. The latter category means streamlining and pushing authority downward, integrating sensors and analysts, thinking of technology as a force multiplier, "need to share," often informally, and becoming more "purple" – that is, more joint in training and exchanges within the intelligence communities but also with consumers.

There is still a long way to go, and it will require intelligence to demonstrate that while we may at times be lying, stealing and deceiving, we are doing this for a purpose and with a mandate, with "minimum trespass" on the privacy and liberties of citizens, in R.V. Jones' words. The process of change and adapting to the new (and itself changing) environment requires skilful leadership. We must understand that success is not guaranteed – we are risking failure and the ensuing "showers of criticism," also a Jones phrase, when things go wrong. It is at those moments when we will most depend on the trust we have built through excellent work.

Panel 1: Emerging Intelligence Fields. While the established intelligence triad (national/transnational security, law enforcement, business/competitive intelligence) is transforming and adapting to new threats and opportunities, and to new demands from users, new intelligence fields with new actors are taking shape in several traditionally non-intelligence or even anti-intelligence environments. This implicit, often unstructured process needs to be analysed in order to increase understanding of the evolution of the social role of intelligence.

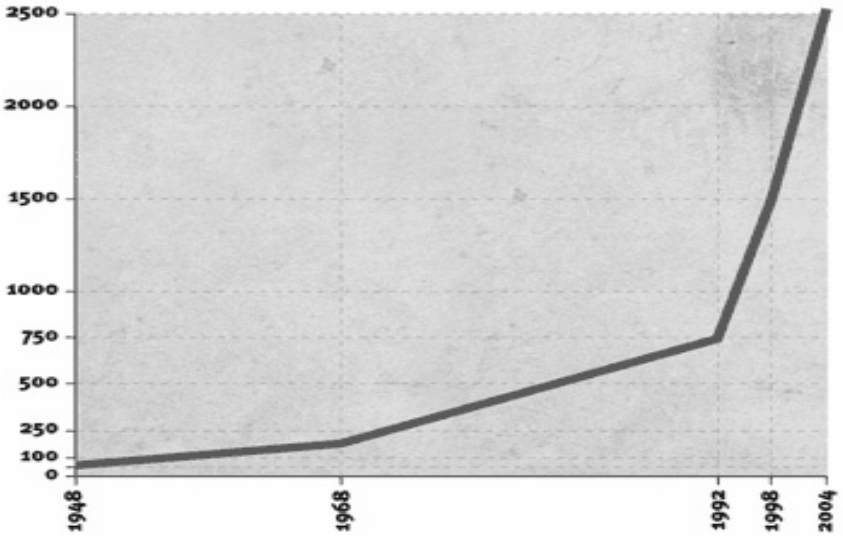
Furthermore, some of these fields contain untraditional intelligence actors, producing and disseminating intelligence and making use of intelligence support in ways not simply copied from the intelligence triad. So, taking the evolutionary nature of intelligence seriously, the emerging fields might have something to offer traditional intelligence in terms of new perspectives on system structure, employment of sources and analytic methods. The starting point is Stevan Dedijer, a guru to some in the room, who recognized ahead of his time that all organization would have to have intelligence is they were to survive. He was ahead of his time in noting the force of the information explosion fifteen years before the Web, along with the power of globalization. As Madonna might put it: "We all live in an intelligence world."

Private sector. In finance there are no remaining borders except currencies, but those cause crises, as they did in Asia in the 1990s. As a result, one bank developed a warning system based on a set of statistical indicators – and formalized it into a signal system. Since it was a business, the process had to raise productivity by economizing on manpower. It was hard, though, to identify the proper market: currency traders have shorter time horizons than the 18 months of the system. Moreover, in that period governments could correct the situation, which meant that only one in three warnings eventuated into an actual currency crisis. This was not helpful in marketing. As a result, the warning was broadened to include the risk of policy tightening – for instance, by increases in interest rates. The warning became that a crisis was likely *if* no tightening occurred. And the sale had to be made to the traders' managers, not the traders themselves.

The basic system is computer-based and one without frills, and so is relatively cheap; add-ons, like textual analysis from Oxford Analytica, are planned and will increase the price – and profitability. Now, the system tracks thirty-five countries with 16 indicators which are updated monthly, looking for changes, or unusual patterns – the "green ribbon turning red." Along the way, the enterprise has learned one powerful lesson for intelligence as well: it is imperative to listen to consumers, in this case for instance in adding countries, or the analysis from Oxford Analytica.

Non-government organizations (NGOs). NGOs now constitute a huge "market" in many sizes and shapes. Figure 1 illustrates the explosive growth of NGOs, tripling in number over the last fifteen years.

Figure 1: NGOs with Consultative Status at the UN



A new generation is more professional and needs intelligence. NGOs need intelligence for a wide range of purposes:

- Exposing violations
  - Gathering evidences and testimonies
  - Identifying perpetrators (States, war criminals)
  - Describing illegal practices (pollution, exploitation, corruption)
  - Understanding patterns of violations
- Assessing humanitarian situation
  - Assessing humanitarian needs
  - locating victims
- Analyzing environment and ensuring security of operations
  - Staff
  - Assets
  - Programs

In this workshop, the focus was on intelligence for the NGO version of "force protection" – protecting NGO staffers in difficult countries. One challenge is that several audiences watch any action, and so a campaign against genital mutilation in Oslo will also be seen in Mogadishu, and thus might become the detonator of protest in the latter.

The list of lapses by NGOs in analyzing the environment ran intriguingly parallel to those for governments. It included stereotypes – the Afghan resistance was "freedom fighters" in one context, terrorists in another; unilateral sources; false categories; distortions across cultures; unquestioned assumptions and unverified information; prejudice and mind-sets; projections; groupthink; too much power to precedents; simple information overload; disinformation; and the pursuit of false consistency.

The NGO world now has more access to technology and talent, and it retains the flexibility that gives it an advantage over governments. Two phones calls produced a meeting for an NGO with Al Qaeda in Sana'a, where the NGO could talk directly about its vulnerabilities. In that sense, NGOs have an opportunity to manage the threat they face, though that invokes hard choices about their "national" identities. For instance, the more visibly "American" one organization might be, the more likely it was to become a target of Al Qaeda.

The analytic toolkit of the NGOs is familiar. Interestingly, what they often feel they lack runs parallel to government. They lack deep expertise in particular countries, and they also lack analytic capacity. They process in which they participate also involves competition – both for donors and for visibility. To be sure, on the ground they often cooperate, and they tend to share an interest in what might be called "radical transparency," but their relations are also competitive.

Organized crime. Organized crime may not be all that organized, and states are very resilient by comparison. September 11th was devastating but hardly an existential threat to the United States. By comparison, organized crime lives in a state of total war; it is Darwinian. This proposition seemed to turn the conventional wisdom on its head, for it is now often thought that networks are more resilient. The old mafia had loyalty rooted in ethnicity; now gangs are different. The individual cells may be brittle, but they can also go elsewhere and start a new gang.

Crime's positive intelligence focuses on opportunities. A half century ago armoured cars were such an opportunity; now it might be a drug shipment or a rival gang that is in trouble. Security is critical, both from the law and from other gangs. Going along with a major police operation one early morning in Newark, it was plain that almost every young newspaper seller along the route immediately called someone to report that the police were out. Organized crime had hired them as spotters. Turning or buying insiders is even more important. And so is security from rival gangs, which seldom is on the radar of law enforcement at all.

In both these senses, intelligence is not a specific role but rather is everyone's responsibility. Everyone keeps his eyes open. The focus is tactical and

low level. What is gathered has to make a difference pretty soon; the pay-off can't be distant. Collectors and analysts and users are all the same. Intelligence becomes, on the one hand, almost a commodity. Yet, on the other, in the closed world of organized crime – it was, after all, La Cosa Nostra ("our thing") – intelligence also confers status.

In that way, intelligence is very individualized. It is held by individuals, and there is little training. Thus, one result is lots of duplication and wasted effort. There is no cycle and little tasking. But neither is there any collecting or producing of information for its own sake. In a world of few constraints, having the reputation for violence can be a benefit.

What has changed is specialization. The Russian gangs came into being as networks, while by contrast the traditional mafia was pretty hierarchical and geographic. Other gangs have adapted by hiring "consultants," for instance, sub-contracting cyber. All this has increased the priority of counterintelligence and of concern over "trace back" – that is obvious with cyber crime. Yet the mystique of secrecy and innovation remains. The intelligence of organized crime is amateur and ad hoc but pretty effective. Failure can mean catastrophe, not just losing money but losing lives.

To what extent do government face similar problems of loyalty if the best analysts move to the private sector? There is little loyalty there: witness Silicon Valley where the best move from company to company for new challenges every few years. If organized crime is changing, so is society. The boundaries are fuzzy. Look at piquem.com, where people can design their own bets. Money is driving, along with excitement, street "creds," not loyalty to organizations or to the state. Yet, by contrast, what drives that U.S. defense analyst to join an NGO, to make even less money, is commitment and perhaps visibility. Surely it would be dangerous if the state itself became too fuzzy, if it were outsourced.

Finally, the discussion picked up a continual theme of the two days – the relative features of different types of intelligence. It seems easier to integrate across roles for operational than for strategic intelligence. Consumers may be harder to engage in strategic intelligence. And doing it well is hard. The British Serious and Organized Crime Agency is a case in point. It didn't fare well, for it turned out not only that the criminal it identified were hard to catch, but that the network analysis on which the agency relied was itself flawed. Sometimes the individuals that seemed critical nodes were more the "secretaries" of the crime organizations than their leaders.

Dogs that Didn't Bark. The idea here was to explore assessments or predictions that *didn't* come true, in contrast to the usual post mortems that explore why it is that events that did occur went unpredicted. For starters, a few examples and the reasons the dogs didn't bark might include, first, the fact that warning

was heeded, hence the predicted danger avoided. There surely was some of that in the famous predictions about Y2K, which didn't come true. That case might also have been averted because of a second factor, that is, mirror imaging. Many of the processes, like running oil refineries, that were complicated and automated in the rich countries were much more labor intensive in most of the world. There, people could simply be hired to turn switches when the millennium turned.

Wishful thinking seems the culprit in other cases, like, most recently, the hope that the protests by monks would topple the repressive government of Myanmar. Sadly, the government didn't seem to get the message. A related failing may be *predicting convenience.* In 1981 the Western world was ready for the Soviet Union to invade Poland. That surely was not the best outcome, but it was perhaps the most convenient one; it was the one for which the Western countries were prepared. When the Poles did the repression themselves, that outcome was probably "better" from the perspective of the West but surely less convenient.

In still other cases, dogs may not bark because of missing indicators or unknown factors. Sometimes, technical failures may contribute to dogs not barking. In other cases, models may be applied to situations in which they are inappropriate; wars in Ethiopia seem to have that character. In more familiar cases, when dogs don't bark, then later predictions of barking dogs are harder to make credible. That was the case with the outbreak of the Korean war, which was predicted a number of times when it didn't occur. Then, two weeks before the outbreak, there was very good warning, which was discounted all around.

The Soviet "war scare" of the 1980s, when Moscow seemed to believe that the United States was about to attack, seemed in part a case of missing indicators. It also, though, suggested another factor – that is, the agendas and budget interests of participants. In that case, both some senior leaders and the military had reason to want to whip up war fear. So, too, part of the Soviet decision to invade Afghanistan reflected the Soviet KGB resident and ambassador seeking to upgrade their statuses by warning that Afghanistan was about to make a deal with the United States.

Panel 2: Dealing with "Complexities." Most intelligence questions about states fell, and fall, into the frequently used distinction between puzzles and mysteries.[1] Puzzles have an answer in principle; intelligence just may not know it. North Korea has X nuclear devices. Mysteries are future and contingent,

1 On the distinction between puzzles and mysteries, see Gregory F. Treverton, "Estimating Beyond the Cold War," *Defense Intelligence Journal*, 3, 2 (Fall 1994); and Joseph S. Nye, Jr., "Peering into the Future," *Foreign Affairs*, 77, 4 July/August 1994, 82-93. For a popular version, see Treverton, "Risks and Riddles," *Smithsonian,* June 2007

with no definitive answer even in principle. Whether North Korea will dismantle its nuclear programs is a mystery. But mysteries have some shape; we know what variables matter most in producing an outcome, and we may have some historical evidence about how they interact. "Complexities," by contrast, are mysteries-plus. [2] Figure 2 displays the range from puzzles to complexities. Large numbers of relatively small actors respond to a shifting set of situational factors. Thus, they do not necessarily repeat in any established pattern and are not amenable to predictive analysis in the same way as mysteries. Those characteristics describe many transnational targets, like terrorists – small groups forming and reforming, seeking to find vulnerabilities, thus adapting constantly, and interacting in ways that may be new. The challenge for intelligence is what, if anything, it can say about complexities that will be useful to a range of consumers from senior policy-makers to police on the street looking for clues to suspicious behavior.

Figure 2: Puzzles, Mysteries and Complexities

Type of Issue	Description	Intelligence Product
Puzzle	**Answer exists but may not be known**	***The* solution**
Mystery	**Answer contingent, cannot be known, but key variables can along with sense for how they combine**	**Best forecast, perhaps with scenarios or excursions**
Complexity	**Many actors responding to changing circumstances, not repeating any established pattern**	**"Sensemaking"? Perhaps done orally, intense interaction of intelligence and policy**

Complexity, Sensemaking and Organization Theory. Taking the Dedjer proposition seriously, all organizations have intelligence. And intelligence is led by leaders. On that score, organization theory has posited three kinds of leaders over the last century. First was the "great man," then a second generation that was less tightly coupled, with bureaucracy having an existence independent of

2 The terms is from Dave Snowden, "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness," *Journal of Knowledge Management*, Special Issue, September 2002, available at http://www.kwork.org/Resources/snowden.pdf, (last visited December 17, 2003). His "known problems" are like puzzles and his "knowable problems" akin to mysteries.

great man (or sovereign). Current notions of leadership are still more decentralized and strategic. The current U.S. Project on National Security Reform is seeking to pull notions away from George Bush's "I am the decider."

Along with those generations of ideas about leadership has gone an evolution in thinking about organizations and strategy. Earlier strategies focused on either cost leadership or product innovation and differentiation. Now, the focus is on high reliability organizations. In Washington, too often all the attention goes to the *strategic level* – Secretary Rice's "big things" – not on the more mundane levels of tactics or operations. Business, though, is just the opposite, talking of the "macro-strategic" to the "micro-strategic," with the latter more important, especially in creating high reliability in organizations. In the financial example discussed earlier, the assessment tool was moved to deal directly with the company's risk assessors, not to report through the CEO.

The earlier focus on organizational structure had ceded pride of place to process. *How* is strategy made? Intelligence is the core of strategy making. Decision-making is embedded in strategy in the sense that strategy may be inferred from watching the decisions that get made. Sensemaking grows out an effort to learn from the past but make sense of the future. The U.S. Army, for one organization, has created a culture of lesson learning through continual post mortems.

By these lights, intelligence is not a constant. It, like sensemaking, should be conceived as a series of episodes, moving from relative order to the chaos of crisis or uncertainty, to another relative order. It is, however, based on an outmoded notion of leadership, one that locates leadership primarily at the top of organizations.

Complexity and Asymmetry. The shift to transnational threats might be thought of as the transition from Cold War 1 to Cold War 2. The first was characterized by a small world with large threats, like nuclear war, on the one hand, and ideological coalitions that produced "chains of dissymmetry" on the other. By contrast, the Cold War that can be dated from September 11th is one of a large world with small, hard to identify threats, on the one hand, and, on the other, the absence of stable ideological coalitions that instead lead to asymmetric campaigns. In one sense, asymmetry is the normal condition of international politics, but it does mean than intelligence can think in terms of behavior but rather must concentrate on behaviors.

Asymmetry relies on the incongruous. It is smaller forces, more cunning, more networked, more prepared to use terror as a tactic. Above all, it recognizes the political nature of war. It is not to be confused with dissymmetry; guerrilla tactics are not an answer to asymmetric threats. Alas, so far there have been too many papers and too few experiments on the battlefield. What the

forces really need is "cheap, fast and out of control." Asymmetric opponents are defeated not by brute force but rather by the ability to systematically deter and discourage opportunistic attacks. That implies systems that are easy to deploy, fast to retreat, transportable by a single man or small unit, and smart, but not too smart.

What are the needs? What future does it mean? Information is pervasive and is a critical tool against asymmetric threats, but it is hard to integrate with regular warfare, with the "system of systems." That takes states back to political warfare, at which they are not so good. Asymmetric forces are exploiting civil vulnerabilities, and the technological solutions that states design are not appropriate for asymmetric conflict. The responses surely cannot be military only

Casualties, psychological effects are a political priority, and take policy into terrain like the media and information warfare – both of which are a "pain in the neck." New policies don't make a difference if the tools are the same.

A not so bright future could be sketched, one in which, as is often observed, technologies are reaching asymmetric opponents. That said, China, India, Palestine, Iraq, Iran and Afghanistan have growing vulnerabilities, but so do France, Germany, and Britain. Those asymmetric opponents need to be addressed across space, with real time mapping of psychological impacts of media warfare and very precise tracking capabilities of fast moving groups blended in the population, using HUMINT and SIGINT in new ways and new combinations.

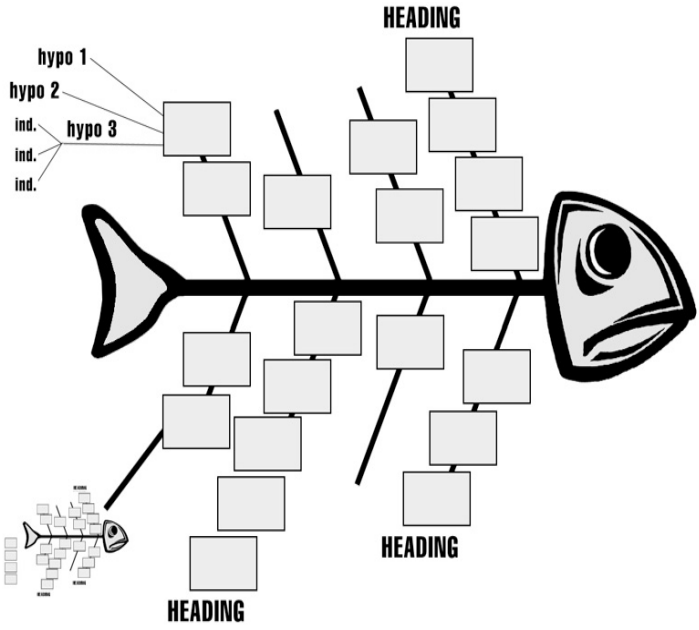
Intervention might take the form of non-lethal directed energy weapons with astounding effect on immediate surroundings and Dust V2.0, parachuted sensors with video capabilities for urban discretionary strikes. All this, though, puts demands on command and control. What is needed is a civil information warfare control room capable of addressing simultaneously civil contingencies and military targets. In the end, thinking about what will deter asymmetric threats may have something in common with thinking about deterrence for criminals. In that parallel world of criminals, as an example, jail time is not deterrence but rather "street creds," with cell phones to make sure business continues to be done.

Approaching Complexities in Organized Crime. The emphasis on "intelligence led" policing came out of Kent, England a generation ago. The logic was that it was better to prevent the 21st crime than to solve the twenty that came before. In that sense, what has been going on is a long experiment at whether that proposition can be made to come true. The challenge is that police generally are inclined to make any case they can, rather than deferring to take up particular cases or concentrate on prevention.

The EU defines organized crime as more than two people engaging in serious criminality with some permanence, where the goal is power or financial gain. The definition is elaborated, but that is the core. Types of crime are less useful as a category, for those tend to remain relatively constant; what police need to focus on is behavior. In that sense, the police live not in a world of limited information but in one of huge information; the problem is relevance. As an example, investigations are law enforcement's main tool, but the critical information is hat is *not* in the investigation. From a police perspective, justice ministries include many "integrity huggers" who make it hard to get at some information that is in police registers.

Much of what passes for "strategic analysis in law enforcement is too general to be helpful – "the price of heroin in falling in Russia," for instance, which doesn't really help local law enforcement in Sweden. The goal of this analysis, rather, is to establish some priorities. It seeks to work in both directions up and down a ladder, both from the top down with seven strategic areas, both regional and functional (Balkans, eastern Europe, human smuggling, cocaine, criminal organizations (prison or motorcycle gangs, for instance), and from the

Figure 3: Mapping Associations and Hypotheses[1]



1 Niki Ekman (2008)

bottom up through known or suspected criminality among groups or individuals. The time horizon is about three years. One Swedish gang began as the Muslim Brotherhood, but then become the "Original Gangsters"; its leader was described as better in jail – both safer and more able to lead. Sometimes honor is more important than turf; for reasons more of the former kids in Gothenburg took on the Bandidos criminal gang.

The process begins with a very open-ended brainstorming, with stickies on a whiteboard, looking for groups and associations. Once that board is full, then the "fish," in figure 3, begins to organize that brainstorming:

The fish metaphor is that tasking is illustrated by the tail, the backbone keeps it all together and the result comes out through the mouth. As the figure suggests, competing hypotheses are added, and one set of associations (in one fish) might be decomposed into a separate fish of hypotheses and associations. The process pays particular attention to resources and capabilities, which are key, as well as the legal business in which crime groups are engaged. It also looks at countermeasures that particular gangs take, like throwing away their cell phones or carefully reading court documents for hints about investigative strategies. Secondary criminality is also important because, on the Al Capone principle, it may be a way to get criminals off the street even if they cannot be caught at their major crimes.

Ideally, one output of the process would be indicators, which could then be fed back as tasking or things to look for. On the whole, though, the people on the street know suspicious behavior, though there are sharp differences among organizations; Custom may notice but the Coast Guard less so.) Observations relevant to those indicators get put in the criminal intelligence register. The main outputs are targeting and priority setting. (In language, law enforcement in Sweden finds it necessary to talk of "problem," for "threat" is the province of the military.) The point is not "strategy" in some grand sense but something more operational. That includes sharing information through the register with those who can use it.

In some ways, it was easier to penetrate the Italian gangs, for they were ethnic and somewhat territorial. While technology lags the needs, sometimes help comes in strange ways. The recent riots in Copenhagen sparked by what Muslims regarded as provocations were bad for business, including criminal business, so the Black Cobra gang discouraged the rioters. Is there risk of a gang-geek alliance? So far, the answer seems less in crime than in terrorism. Gangs have not used the Web as a recruiting device to the same extent, but rather have relied on it more for communication.

APPENDIX

Center for Asymmetric Threat Studies
New Frontiers in Intelligence

Workshop Program and Goals

May 27-28, 2008

Workshop goals: To look in depth at two key frontiers for intelligence in an era of terror: 1) To understand and learn lessons from new and non-traditional fields of intelligence and new actors, from non-governmental organizations (NGOs) to organized crime; and 2) To address intelligence "complexities" – that is, issues or threats, like that of terrorism, that may involve large numbers of relatively small actors responding to situational factors that do not necessarily repeat established patterns.

Background: This workshop will address two central themes in the CATS project: new actors and emerging intelligence fields, and dealing with "complexities" – both directly relevant to terrorism and homeland security.

Emerging intelligence fields: While the established Intelligence triad (national/transnational security, law enforcement, business/competitive intelligence) is transforming and adapting to new threats and opportunities, and to new demands from users, new intelligence fields with new actors are taking shape in several traditionally non-intelligence or even anti-intelligence environments. This implicit, often unstructured process needs to be analysed in order to increase understanding of the evolution of the social role of intelligence.

Furthermore, some of these fields contain untraditional intelligence actors, producing and disseminating intelligence and making use of intelligence support in ways not simply copied from the Intelligence triad. So, taking the evolutionary nature of intelligence seriously, the emerging fields might have something to offer traditional intelligence in terms of new perspectives on system structure, employment of sources and analytic methods. The purpose of this session is to make a first cut into this field of non-traditional intelligence, with a presentation of examples of new actors and how they perceive their intelligence systems and purposes.

Dealing with "complexities": Most intelligence questions about states fell, and fall, into the frequently used distinction between puzzles and mysteries.[3] Puzzles have an answer in principle; intelligence just may not know it. North Korea has X nuclear devices. Mysteries are future and contingent, with no definitive answer even in principle. Whether North Korea will dismantle its nuclear programs is a mystery. But mysteries have some shape; we know what variables matter most in producing an outcome, and we may have some historical evidence about how they interact. "Complexities," by contrast, are mysteries-plus. [4] Large numbers of relatively small actors respond to a shifting set of situational factors. Thus, they do not necessarily repeat in any established pattern and are not amenable to predictive analysis in the same way as mysteries. Those characteristics describe many transnational targets, like terrorists – small groups forming and reforming, seeking to find vulnerabilities, thus adapting constantly, and interacting in ways that may be new. The challenge for intelligence is what, if anything, it can say about complexities that will be useful to a range of consumers from senior policy-makers to police on the street looking for clues to suspicious behavior.

3 On the distinction between puzzles and mysteries, see Gregory F. Treverton, "Estimating Beyond the Cold War," *Defense Intelligence Journal*, 3, 2 (Fall 1994); and Joseph S. Nye, Jr. , "Peering into the Future," *Foreign Affairs*, 77, 4 July/August 1994, 82-93. For a popular version, see Treverton, "Risks and Riddles," *Smithsonian,* June 2007

4 The terms is from Dave Snowden, "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness," *Journal of Knowledge Management*, Special Issue, September 2002, available at http://www.kwork.org/Resources/snowden.pdf, (last visited December 17, 2003). His "known problems" are like puzzles and his "knowable problems" akin to mysteries.

DAY 1

12:00 **Lunch**

1:00 **Introduction to workshop**
Lars Nicander, CATS
Gregory Treverton, CATS and RAND Corporation
Wilhelm Agrell, CATS and Lund University

1:15 **Setting the Challenge for practitioners: Intelligence, Law Enforcement and the Changing Threat**

Christian Jenny, Swiss Federal Department of Defence, Civil Protection, and Sports, Secretariat General

What does the problem, especially the intelligence problem or the analytic problem at the intersection of intelligence and law enforcement, look like from a practitioner's perspective? What are the special challenges of this period, and of the terrorist target in particular? And how might thinking or research lead to improvements in practice?

1:30 **panel 1:** ***Emerging Intelligence Fields***
Panel presentations from the following perspectives:

- NGOs, which tend to be uncomfortable about "intelligence' and "government but which do have their own intelligence systems;
- Government inspectors of finance or insurance: what do they look for, what is their "system"?
- Intelligence "entrepreneurs": private companies, often run by ex-intelligence operations officers. What do they offer? How do they think about their "intelligence" tasks?
- Organized crime, some of which plainly has very good intelligence: what are we missing, what might we learn? Hackers and cybercriminals might be a special example.

Panellists

- Wilhelm Agrell
- Rutger Palmstierna
- Pascal Daudin, Care International, Switzerland
- Mark Galeotti, University of Keele, UK:

3:15 **break**

3:30 ***Discussion***

This discussion will compare and contrast the different emerging fields. What might be learned from each? What is the relationship of each to more traditional intelligence? Are there common themes, practices or approaches across the very different emerging fields?

5:00 ***Wrap-up***
Wilhelm Agrell
Gregory Treverton

DAY 2

8:45 **Introduction to panel 2: Addressing "Complexities"**

Gregory Treverton, CATS and RAND Corporation

9:00 **What Are Complexities, and What Challenges Do They Pose for Intelligence**?

Panel presentations from the following perspectives

- Defining complexities: What are they, and how do they differ from puzzles or mysteries? Are they especially prevalent in terrorism and other transnational issues; if so, why? What, realistically, can intelligence offer to policy with regard to them?
- Dealing with complexities in crises, national security or the private sector: What problems are complexities in other domains? What are their characteristics? What is "sensemaking with regard to them? What are the particular challenges?
- Complexities, sensemaking and Intelligence: How do practitioners conceive of complexities, even if they do not label them that? What processes or methods do they use to make sense of them? What does intelligence owe policy when it may not be able to reduce uncertainty by very much?

Panellists

- Gregory Treverton
- James Douglas Orton, George Washington University, USA
- Philippe Baumard, University Paul Cezanne, France
- Niki Ekman, National Criminal Police, Sweden

10:45 break

11:00 Discussion: Predicted Dogs that Didn't Bark

This discussion will ask what might be learned from predicted events that did not happen. Here the list might be as wide as the Y2K disaster that passed almost without notice; the AIDS global pandemic that wasn't; the 1981 Soviet invasion of Poland that didn't happen; and, especially, the "small" but crippling terrorist attacks – like several simultaneous suicide bombings at shopping malls – that haven't come. What are we missing? Is any thread common across these non-barking dogs? Is complexity any part of the reason why they didn't happen? What about blue – that is, "us": did intelligence's ignorance of, or inability to explicitly include what was going on in government policy or private sector action at home play any part?

12:15 Wrap-up
Gregory Treverton
Wilhelm Agrell

12:30 Lunch

Panellist Bios

Wilhelm Agrell is historian and professor in intelligence analysis at Lund University, Sweden. He has studied the role of Sweden in Allied intelligence operations during the Second World War and the Scandinavian segment of the Venona decrypts.

Philippe Baumard is currently associate-researcher to the Orange – France Telecom Chair on Innovation and Regulation of Numerical Services at the Ecole Polytechnique, Center for Management Research. He is also Executive Advisor to EADS Corporate R&T Innovation Works. A Visiting Professor with the Haas School of Business (2004-2007), University of California, Berkeley, Institute of Business and Economic Research, Professor Baumard works focus on the dynamics of technological innovation, unlearning and strategic change. A former Director of Strategic Studies for the France Telecom, and Strategy Advisor, his work is grounded in the transformation of large corporate organizations facing strategic reorientations and swift change of economic and strategic models. A fellow of the Paris-Oxford Chancellors Grant, Prof. Baumard has graduated in Social Sciences (History and Sociology) from ENS-EHESS, University of Paris-Dauphine (PhD), and has been a visiting faculty at the University of Lund, Sweden, New York University, University of Technology, Sydney, Oxford University, and UC Berkeley. A early contributor to theories and doctrines of information warfare (AFCEA, 1996), he initiated with C. Harbulot the French Commission on Economic Intelligence and Enterprise Strategy, at the French Prime Minister Office of Planning in 1994. He published more than 60 articles and 7 books.

Pascal Daudin is currently Director of Safety and Security Unit of CARE International. After a short career as free-lance journalist he joined the International Committee of the Red Cross in 1985 and has occupied various positions of line manager and protection expert as well as humanitarian law specialist. During his 16 years term with the organization he was deployed in major conflict situations such as Afghanistan, Lebanon, Iraq, Iran, Central Asia, Caucasus and the Balkans. After leaving the ICRC, he worked as senior analyst and deputy-head of a counter terrorism unit attached to the Swiss Ministry of Defense. Since 2007, he 'is in charge of all matters related to security issues concerning CARE International Operations and institutional responsibility. He holds a master in International Relations and has obtained various diplomas in Human rights and Humanitarian law.

Niki Ekman presently works at the National Criminal Police where she is deputy head of the Criminal Intelligence Section. She started the Police Academy in 1978 and did the usual 10 years in uniform. During this time she studied law and she received a Master of Law from the University of Stockholm in 1987. In 1995 she was recruited the newly formed National Criminal Intelligence Service, where she specialized in strategic intelligence analysis. In December 2000 she received a Master of Science in Administration of Justice with a specialty in Research, Intelligence Analysis from Mercyhurst College in Pennsylvania USA.

She lectures extensively on the subject of criminal intelligence analysis.

Mark Galeotti is the Director of the Organised Russian & Eurasian Crime Research Unit (ORECRU) and head of the History department at Keele University, UK. He read history at Cambridge University and then took his doctorate in politics at the London School of Economics. He has been based at Keele since 1991, although he was seconded in an advisory role to the Foreign & Commonwealth Office, 1996-97, where his remit covered post-Soviet organised crime and the Russia security and intelligence services, and he was visiting professor in public security at Rutgers-Newark, USA, 2005-6. He has published widely, with 10 books to his name and wrote a regular column on post-Soviet affairs in Jane's Intelligence Review 1991-2006. He is the Founding Editor of the journal *Global Crime* and European Editor of *Low-Intensity Conflict & Law Enforcement*. He also has widespread consultancy experience, with clients ranging from governments and law-enforcement agencies (including the British National Criminal Intelligence Service and Interpol) through to commercial clients. He has given evidence before the House of Commons Foreign Affairs Select Committee and briefed officials from numerous British and foreign government departments.

Dr. Christian Jenny is Head of the Terrorism Analysis Branch with the Secretariat General of the Swiss Ministry of Defence, Civil Protection and Sports (DDPS). He has worked with the DDPS for 14 years, first as an analyst on Counter Proliferation issues, and since 1999 as branch head. He joined the DDPS after studies in History, Constitutional Law and American Literature at the Universities of Berne and Michigan, writing a dissertation on the origins of Austrian neutrality. Christian holds a reserve commission as lieutenant colonel with the Swiss Air Force.

Lars Nicander is Director for The Center for Asymmetric Threat Studies at The Swedish National Defence College. He was between 1997-2002 appointed Secretary of the Cabinet Working-Group on Defensive Information Operations. A political scientist by training, he has served in various positions within the Swedish national security environment. He is an elected member of the Institute of Strategic Studies in London (IISS), a Fellow of The Royal Swedish Academy of War Sciences and also belonging to the Board of Advisors for the Terrorism Research Center, McLean, Va.

James Douglas Orton (Ph.D., University of Michigan) is a senior organization and management theorist for the Project on National Security Reform., a non-partisan system reform project funded by the U.S. Congress through the Defense Authorization Act of 2008. Dr. Orton has a long-term applied research and executive education relationship with The George Washington University Executive Leadership Doctoral Program (1994-2008), where he teaches doctoral seminars on organizational leadership, organizational structure, organizational culture, organizational strategy, organizational decision-making, organizational learning, organizational sensemaking, organizational change processes, and high reliability organizations. He has taught similar doctoral seminars at Boston College (1990-1994), HEC Paris (1994-2000), MIT (1998), and UC-Irvine (2003-2004). Dr. Orton is an expert on loosely coupled systems, organizational sensemaking processes, high-reliability organizations, and national security management processes.

Rutger Palmstierna joined the Swedish Foreign Service in 1970, after having studied classical languages at high school and Chinese at university (on top of political science and economics, as well as an MA at the London School of Oriental and African Languages), After postings to Geneva, Bonn, Beijing and Jakarta in the 70's, he worked at the MFA in Stockholm, first on international nuclear energy matters and non-proliferation of nuclear weapons, and then on international debt restructuring. In the latter capacity he took part in the 1980's resolution of the East European and Third World debt crises, which

earned him an invitation, in 1986, to join SEB, Sweden's most international bank. From 1991 he had, as a member of the bank's country risk committee, sole responsibility for the bank's country risk analysis. This task necessitated a development of structured methods to assess and rate political risk in which he developed successive generations of country risk assessment and rating systems.

In 2000 he returned to debt negotiation matters as an advisor to the Government of Moldova on external debt until the debt issues resolution in 2006/07. At 2001/02 he retired from SEB and formed his own company Macro Intelligence, the core business of which is the Macro Intelligence Early Warning System (MIEWS) that he agreed with SEB to bring with him.

Gregory Treverton is director of the RAND Corporation's Center for Global Risk and Security, as well as a visiting fellow at CATS. Earlier, he directed RAND's Intelligence Policy Center and its International Security and Defense Policy Center, and he was associate dean of the Pardee RAND Graduate School. He has served in government for the first Senate Select Committee on Intelligence, handling Europe for the National Security Council and, most recently as vice chair of the National Intelligence Council, overseeing the writing of America's National Intelligence Estimates (NIEs). He holds an A. B. *summa cum laude* from Princeton University and an M.P.P (Master's in Public Policy) and Ph.D. in economics and politics from Harvard. His latest book is *Intelligence for an Era of Terror,* forthcoming from Cambridge University Press.