Intelligence and Prediction in an Unpredictable World

CISAC

June 20-21, 2003

sponsored by the
Center for International Security and Cooperation
Dwight D. Eisenhower National Security Series

Intelligence and Prediction in an Unpredictable World

Part of the U.S Army's Eisenhower National Security Series

Summary by Todd S. Sechser

On June 20 and 21, 2003, the Center for International Security and Cooperation (CISAC) at Stanford University hosted a workshop on intelligence problems facing the United States in the areas of terrorism and nuclear proliferation. The workshop, which brought together approximately 75 scholars, intelligence and policy practitioners, and scientists, was co-sponsored by the U.S. Army as part of the Eisenhower National Security Series.

Key Insights:

- The intelligence community should improve its ability to share relevant intelligence across domestic- and international-focused agencies and between U.S. and foreign intelligence agencies.
- "Mirror-imaging" in intelligence assessments can lead to false inferences about motivations and likely behavior. Analysts should not use the U.S. nuclear experience to draw inferences about a country's motivations and decisions.
- Proliferation analysts should keep in mind that weapons decisions are often made under conditions of deep bureaucratic division and do not necessarily reflect a consensus on national goals.
- Intelligence analysts face strong incentives to err on the side of overly pessimistic predictions because "crying wolf" is rarely punished. These incentives must be structured properly to avoid numbing policymakers with worst-case threat assessments.
- U.S. counter-terrorist intelligence should give more priority to learning about the organizational characteristics of terrorist groups.
- Intelligence analysts often lack deep knowledge of U.S. policies and thus fail to recognize how U.S. policies will influence the behavior of the government under consideration.
- Excessive attention to intelligence failures often inhibits the efforts of analysts to devise broader strategies for predicting proliferation. Focusing on small intelligence shortcomings may undermine long-term strategy-building by setting improper standards for strategy evaluation and comparison.

The workshop was driven by the awareness that a nation's security depends not only on its military brawn but also on its brains: without the ability to predict and plan for likely threats, even the strongest nation is handicapped in its efforts to protect itself. While counter-terrorist intelligence has received much scrutiny in the wake of the September 11, 2001 terrorist attacks, the broader ability of the intelligence community to predict important national security developments has received inadequate attention. The panels described below attempted to remedy this shortcoming.

PANEL 1: Terrorism and Intelligence: September 11 and Current Challenges

Conventional wisdom in the wake of the September 11 terrorist attacks in New York and Washington, DC holds that the attacks were enabled by a massive intelligence failure on the part of the United States. Is this view correct? What can intelligence agencies be reasonably expected to know and not know? To what degree are we "preventing the last attack" in our counter-terrorism efforts? These and other questions motivated the workshop's opening panel.

The panel began by considering the nature of the terrorist threat to the United States. Most agreed that al Qaeda poses a uniquely serious threat to the United States. The organization's tight operational security and flexible, decentralized command structure make penetration by intelligence agents difficult, while its interest in weapons of mass destruction (WMD) raises the urgency of its threat. (Disagreement existed, however, about whether terrorist groups are likely to execute a successful WMD attack in the near future.) Although its prior safe haven of Afghanistan is gone and many of its leaders have been killed or captured, it nevertheless continues to operate near the border of Afghanistan and Pakistan. Furthermore, its top leadership (namely, Osama bin Laden) remains at large and al Qaeda enjoys considerable sympathy and recruiting success in the Muslim world.

More broadly, some panelists emphasized that the growth of theologically-oriented terrorist groups constitutes a new threat that deserves greater attention from U.S. policymakers. Groups such as the Aum Shinrikyo and al Qaeda are driven by a belief in a "divine mandate" and consequently display stronger proclivities toward spectacular, destructive, and often undeterrable attacks.

The panel found itself in broad agreement about three major challenges in countering terrorism. First, intelligence agencies must be structured to use intelligence preventively. Panelists argued that the case-based nature of the FBI's work encumbers its ability to utilize intelligence for preventive purposes: FBI agents are trained to sort information into relevant case files, but most counter-terrorism intelligence does not fit into existing criminal cases. Agents face strong professional incentives to build portfolios in law enforcement – that is, by building cases against wanted individuals for crimes already committed – rather than in preventing future acts of terrorism.

Second, the intelligence community must improve its ability to share relevant intelligence across agencies. Some panelists argued, for example, that the organizational culture of the FBI excessively restricts information-sharing with other intelligence agencies. Moreover, a historic firewall between the CIA and FBI has left a residue of suspicion and non-cooperation that may inhibit the flow of important information to

analysts attempting to "connect the dots" between disparate pieces of intelligence.

Third, intelligence organizations must ensure that they are appropriately designed for these tasks. While interagency rivalry helped protect civil liberties and may have produced healthy competition during the Cold War, it is not clear that a stovepiped intelligence community is an effective means of combating a decentralized terrorist threat.

The discussion also brought a number of uncertainties to light. For example, what tactics is al Qaeda likely to adopt in the near future? Will it shift its attention away from targets that have received security upgrades since September 11 and toward more vulnerable public targets? Perhaps even more intriguingly, why has it not struck against the United States since September 11?

PANEL 2: Intelligence, Terrorism, and Proliferation: Views from Abroad

The first panel's discussion focused on the American intelligence experience, but this session was designed to offer a broader perspective. Do foreign intelligence organizations face problems similar to those of the United States, and how have they addressed these challenges? What lessons can the United States learn from their experiences?

Based on their experiences with foreign intelligence agencies, the panelists considered a wide variety of organizational pathologies that can hamper the collection of intelligence. One such problem is that of "mirror-imaging," in which intelligence analysts make predictions based on what they would do "in the other's shoes." The presumption that the enemy's values and decision-making processes are similar to one's own can lead to disastrous predictive failures. Analysts must be particularly sensitive to this problem when considering likely terrorist tactics – assumptions about terrorists' choices and priorities should be based on real intelligence, not "logical" extrapolations from rationalist assumptions.

Likewise, intelligence can be vulnerable to mirror-imaging in proliferation issues – one should not assume that foreign countries will face technical challenges similar to those of the United States, or that their pursuit of various capabilities implies anything about their motivations. States pursue nuclear weapons for vastly different reasons, and one often cannot deduce the reasons driving a nuclear program without an acute awareness of unique cultural and domestic political factors that may be at work.

Foreign intelligence experiences also teach that policy-makers can influence the type and quality of intelligence they receive by the questions they ask, according to the panelists. Policy-makers that are overly concerned with short-term intelligence, for example, may miss long-term developments because they have not encouraged their intelligence agencies to look for patterns or identify broad trends.

Furthermore, the panel argued that enemies rarely have "grand designs" that drive their every action. A state's acquisition of nuclear weapons, for example, may in reality be driven by a small but powerful political or bureaucratic faction. Assuming that proliferation represents a careful, well-considered strategic choice can lead to false inferences about a state's future behavior.

The panel agreed that the United States could benefit greatly from sharing

intelligence with foreign countries. Some participants questioned whether strict rules of secrecy would make high levels of sharing feasible, particularly when the U.S. intelligence community suffers from insufficient contact among its own agencies. Speakers replied, however, that such sharing already occurs, although they acknowledged that suspicion of foreign motives sometimes inhibits cooperation.

As in the previous panel, some participants wondered aloud about the value of open-source information and criticized intelligence agencies for relying excessively on classified material for drawing their assessments. Panelists replied, however, that open-source information is often politically-motivated and not credible, precisely because the creator of that information knows the other side will be privy to it.

PANEL 3: Organizational Behavior, Terrorism, and Intelligence

New concerns about proliferation and terrorism have sparked increased interest in utilizing organizational theory to understand enemies and ourselves. Protecting against insider threats, reducing the unpredictability of complex systems, understanding organizational learning, and providing coordination between competing organizational units are issues that have been analyzed in other contexts by sociologists and political scientists. What can we learn from them?

Panelists commented first on the need to consider the organizational proclivities of intelligence organizations. A critical insight here was that organizational objectives sometimes diverge from the interests of the individuals that comprise them. In other words, organizations can fail when their members face incentives to act in ways that are not in the interests of the organization. Panelists noted a number of ways that this problem can afflict intelligence organizations.

First, intelligence analysts sometimes face strong incentives to err on the side of predictions that are too pessimistic because failures to predict threats are punished severely, while "crying wolf" is not. The resulting gloominess of intelligence can undermine its credibility and numb policymakers to future threat assessments.

Second, the division of responsibility within organizations influences the degree to which assignments are followed. One panelist offered that adding security guards to nuclear power plants may not improve overall security if individual responsibilities are not clear in the case of a terrorist attack. Indeed, adding guards may actually reduce security if the presence of additional security guards produces "social shirking" in a crisis. Panelists and participants discussed using exercises to obtain data on social shirking and other organizational problems.

Finally, organizations contain layers of unchallenged assumptions that can impede the performance of its duties. One speaker pointed to the failure of the U.S. military to incorporate measurable fire effects into nuclear damage estimates during the Cold War as an example of the process by which fallacious assumptions can become embedded in organizational knowledge. Participants agreed that intelligence organizations must do a better job of challenging and testing the assumptions that drive their predictions.

Conversely, the panel pointed out that the U.S. should consider the organizational

characteristics of terrorist groups when formulating counter-terrorist strategy. Like any organization, terrorist organizations are comprised of components, each of which are susceptible to different tactics. Terrorist organizations contain leaders, lieutenants, foot soldiers, recruiters, suppliers, and state supporters, all of whom have different priorities and can be countered or deterred in different ways.

Taking an organizational view of terrorist groups, according to the panel, would lead to the conclusion that an effective counter-terrorist strategy would focus on: deterring states from providing safe haven and material support to groups like al Qaeda; bolstering U.S. credibility and legitimacy in states that tolerate terrorists' presence (particularly Arab states); and crushing al Qaeda in the short term to convey a message to the foot soldiers of similar organizations.

PANEL 4: Predicting Nuclear Proliferation: Recent Cases and Lessons

John F. Kennedy warned that by the end of the 1960s, perhaps twenty-five nations would become members of the nuclear club. Forty years later, his dire prediction remains only one-third true. Have U.S. intelligence agencies fared any better in their estimates of who would acquire nuclear weapons? Panel members examined both historical case studies of proliferation expectations and the recent record of predictions in South Asia, East Asia, and the Middle East.

One point emphasized by a number of the panelists was the close-knit relationship between intelligence and policy. What may be popularly seen as an "intelligence failure" may in fact be the consequence of a policy that assigns insufficient importance to a particular country or issue.

The panel sparked passionate discussions about the relevance of proliferation-related intelligence for policy-makers. If a state is well on its way to developing or testing nuclear weapons, how much would such knowledge actually alter U.S. policy? Some participants suggested that it would not, arguing, for example, that prior knowledge of India's impending nuclear tests in 1998 would not have permitted the U.S. to prevent them. Furthermore, some claimed that efforts to gain intelligence on the size of North Korea's nuclear arsenal (if it exists) are futile because it would make little difference if North Korea possessed one, a few, or many nuclear weapons – in all cases, it would still be a nuclear weapons state and the U.S. would need to adjust accordingly to this fact.

Others, in contrast, asserted that India's efforts to conceal its 1998 nuclear tests suggested that it would have been susceptible to U.S. pressure if appropriate intelligence had been available in time. Likewise, some panelists suggested that a North Korea with one nuclear weapon would call for very different policy approaches than a North Korea with several weapons (a North Korea with one weapon would be unlikely to sell or test it, while the same would not be true if it had several).

One participant argued that the tendency to see nuclear weapons programs as products of unified, well-considered decisions of national governments sometimes leads to inappropriate policy responses. Nuclear programs are often born amid sharp bureaucratic divisions, and the outcomes of these battles may not necessarily reflect the majority view of the government. This point mirrored comments made during the second panel, when speakers noted the perils inherent in imputing specific motives to efforts to acquire nuclear weapons.

Panelists discussed a common problem with intelligence estimates: the failure of analysts to predict the impact of US policies on the governments they are studying. Better understanding of U.S. policy making among intelligence specialists could reduce the effects of this problem.

A final argument made by one speaker was that excessive attention to intelligence failures often inhibits the efforts of analysts to devise broader strategies for predicting proliferation. All strategies are bound to suffer periodic tactical failures, but the critical question is which strategies perform most successfully over time. Focusing on small intelligence shortcomings may undermine long-term strategy-building by setting improper standards for evaluation and comparison.

PANEL 5: Predicting Proliferation: Looking Back and Looking Forward

In contrast to the specific cases of nuclear proliferation analyzed in the previous panel, this group of scholars attempted to take a broader outlook on the ability of intelligence agencies to forecast the proliferation of nuclear, biological, and chemical weapons. Which variables have proven useful in constructing these forecasts, and which factors have defied expectations by proving to be poor predictors?

The panel began with a historical inquiry into the predictive record of the United States, particularly during the 1960s. One speaker noted that the United States was not caught off-guard by China's test of an atomic weapon – indeed, U.S. intelligence had been predicting the test for some time when it finally occurred in 1964. Subsequent predictions of widespread proliferation, however, were overstated: while American intelligence officials believed that a wave of nuclear acquisitions in Europe, Asia, and the Middle East would follow China's test, proliferation was in fact relatively well-contained. Little mention was made at the time, however, of South Africa, which did build a nuclear arsenal later on.

On the other hand, proliferation intelligence estimates in the 1960s did succeed in questioning assumptions both about motives and capabilities of potential proliferators. One speaker noted, for example, that bureaucratic politics was a key variable in proliferation assessments of the time. The inclusion of such an obscure (but critical) variable made these assessments unique.

Another panelist noted that growing cooperative linkages among proliferators will make nuclear export controls increasingly ineffective and proliferation outcomes much harder to predict. As states develop networks that allow each to specialize in some aspect of nuclear or missile technology, controlling the spread of such technologies will become more challenging. New proliferators are less likely to produce massive and hard-to-hide programs – instead, proliferation will be the result of divided and shared labor among countries whose programs will be less detectable.

The discussion turned to the broader subject of how proliferation-related intelligence and prediction might be improved in the future. Participants agreed that managing uncertainty is the critical challenge of intelligence analysts: because eliminating ambiguity is impossible, analysts must develop tools for characterizing uncertainty in ways that are useful and meaningful for policy makers. Doing so is difficult,

however, because policy makers are rarely satisfied with ambiguity. Nevertheless, one speaker explained, extreme caution in analysis can be costly and should be avoided.

The panel agreed with earlier participants that excessive pessimism is rife in intelligence analysis, largely due to professional incentives to err pessimistically in threat analyses. Some speakers explained that removing such career incentives is essential to improving prediction – those that "cry wolf" must be held accountable as well as those who do not alert policy makers to emerging threats. On the other hand, however, because threats may fail to emerge due to policies that intelligence analysts help shape, punishing those responsible for such assessments may be counterproductive in some cases.

PANEL 6: Roundtable: Predicting and Coping With Future Threats

The final panel cast an eye forward to evaluate the impact of new technological and political developments on the future of intelligence. Have we learned from past successes and failures to organize our intelligence efforts more effectively? To what degree will technological innovations on the horizon truly improve our ability to predict the identities, military capacities, and intentions of potential adversaries? Finally, what will intelligence analysts look to in the future to develop their assessments? Will enhanced detection capabilities affect the way analysts reach their conclusions, or will the process remain relatively constant?

One panelist noted that analysts attempting to predict proliferation in the future will need to pay more attention to the demand for nuclear weapons and rely less on capability assessments. Indeed, it is precisely the increasingly widespread diffusion of nuclear and delivery technologies that will force intelligence analysts to shift their focus away from capabilities and to more political assessments of motivations.

Other speakers followed up by calling for greater creativity and more vigorous questioning of assumptions by the intelligence community. Collecting useful intelligence requires one to look in the proper places, and the threat of terrorism in particular requires an active imagination on the part of the intelligence community – both in envisioning potential threats and in devising responses. Herein lies a critical nexus of intelligence and policy, the panel noted: policy-makers must be imaginative in comprehensively identifying one's core interests, while intelligence analysts must envision possible threats to those interests. Organizational managers thus shoulder a major responsibility in ensuring that organizational members are motivated by more than altruism to utilize their creativity.

The workshop concluded with a shared note of caution: for all the effort and resources that are devoted to prediction and early warning, policy-makers must nevertheless be prepared for prevention to fall short. Emerging threats such as space weapons and biological terrorism will be difficult to detect by even the best intelligence analysts. Intelligence is no substitute for preparation in the event that prediction and prevention fail.

Eisenhower National Security Series
1201 E. Abingdon Drive, Suite 201
Alexandria, VA 22314-1493
Telephone: (703) 254-0047
Fax: (703) 549-0211
E-mail: info@eisenhowerseries.com
http://www.eisenhowerseries.com