



**REPORT OF THE WORKING GROUP ON
RELATIVE THREAT ASSESSMENT**

WORKING GROUP CO-CHAIRS:

Christopher Chyba
*Stanford University**

Harold Feiveson
Princeton University

David Victor
Stanford University

REPORT OF THE WORKING GROUP ON RELATIVE THREAT ASSESSMENT

Christopher Chyba, Harold Feiveson, and David Victor (co-chairs)

Introduction

The working group (see Box 1) defined its task as follows: *How can one improve the utility of threat assessments in the formulation of national security policy?* We have seen our task as putting forward principles that the PPNS leadership should consider when evaluating the various threat assessments that are used to inform national security strategies. We have not conducted our own independent threat assessments. Rather, we have looked to recent history to explore how assessments have been formulated and deployed.

This report reflects the deliberations at three meetings of our working group. It also draws on briefings presented at these meetings, three commissioned background papers, and our own experiences and readings. We did not seek consensus among members of the working group, but we did benefit from their review and critique; this summary report is the responsibility of the co-chairs, although it reflects the tenor of the working group's discussions.

Three commissioned background papers were written by members of the working group. One surveyed nine major threat assessments that have been conducted in the last half decade.¹ A second looked at threat assessments done during the several periods of the Cold War and post Cold War and the interactions between the process of threat assessment and the practice of setting priorities in government.² The third examined a particular type of organizational reform that could lead to better application of threat assessments—an expansion of the Pentagon's quadrennial defense review (QDR) into a broader quadrennial national security review (QNSR).³ All three papers are available on the Princeton Project [web site](#). The threat assessments explicitly examined are shown in Box 2.

Broadly, the PPNS working groups have explored three classes of threats: a) those where there is an identifiable enemy agent, such as a government or a terrorist group; b) those that derive entirely or in part from human action but are not the product of hostile intent, such as climate change, accidental nuclear war, or emerging diseases and c) dangers that stem from natural disasters such as asteroid impacts and earthquakes.⁴

¹ Dara Cohen, *Background Briefing Paper*, March 4, 2005

² Chris Preble, *The Uses of Threat Assessment in Historical Perspective: Perception, Misperception and Political Will*, June 16, 2005.

³ Michèle Flournoy and Shawn Brimley, *Strategic Planning for U.S. National Security: A Project Solarium for the 21st Century*, July 2005.

⁴ There are, of course, other ways to categorize threats. The PPNS working group on State Security and Catastrophic Threats considered three classes of threat: terrorism and criminal networks, disease and bioterrorism, and natural disasters and resource scarcities. The Grand Strategy working group has considered, among other issues, threats categorized by origin—such as the dangers associated with the rise of China or terrorist-jihad organizations. Other working groups have looked at economic threats and the threats arising from anti-Americanism.

Most threat assessments adopt the “classic” approach and focus on the first category—threats that originate in hostile intention. These assessments typically rest on three types of considerations. First, they describe the immediate impacts of an attack by imagining the *capabilities* of the adversary—for example, a terrorist attack on U.S. soil with nuclear or biological weapons, a ballistic missile attack from a rogue state, or a deliberate disruption of Persian Gulf oil exports. Second, they sometimes (though more rarely) include an assessment of adversaries’ likely *intentions*—an evaluation of their worldview, motives, modus operandi, strengths and weaknesses. Third, threat assessments also typically include attention to the *vulnerabilities* of the U.S., including the consequences of a successful attack.

Ideally, a threat assessment should connect these three strands—capabilities, intentions, and vulnerabilities—to provide a full picture of the origins and consequences of actions that threaten U.S. interests. In turn, threat assessment can then be used to set priorities for national security strategy—the investments in resources, political initiatives, and other responses that comprise U.S. policy.

We have wrestled some with the distinction between intelligence analysis and threat assessment. One description of this distinction is that an intelligence analysis provides information about what is happening or might happen in the future. A threat assessment places such information in the context of U.S. interests. The intelligence analyst could, for example, offer an evaluation of the range and accuracy of Iranian intermediate range missiles. A threat assessment would examine how this threat affects U.S. security and how such threats compare with other dangers, informing the development of a strategy to mitigate the threat. The ultimate goal of threat assessment is ideally to set priorities for resources, such as budgets and bureaucratic attention.

BOX 1: Working Group on Relative Threat Assessment

Christopher Chyba, Co-Chair, Stanford University*
Harold Feiveson, Co-Chair, Princeton University
David Victor, Co-Chair, Stanford University
Peter Bergen, The New America Foundation
Coit Blacker, Stanford University
Richard Falkenrath, Brookings Institution
James Fallows, Atlantic Monthly
Ed Felten, Princeton University
Michèle Flournoy, Center for Strategic and International Studies
Jamie Gorelick, Wilmer, Cutler, Pickering, Hale and Dorr
Margaret Hamburg, Nuclear Threat Initiative (NTI)
Robert Hutchings, Princeton University
Jessica Mathews, Carnegie Endowment for International Peace
Michael Meese, U.S. Military Academy
Michael O'Hanlon, Brookings Institution
Elisabeth Paté-Cornell, Stanford University
Chris Preble, Cato Institute
Scott Sagan, Stanford University
Steve Stedman, UN and Stanford University
Dara Cohen, Research Assistant, Stanford University

*Princeton University as of July 1, 2005

We summarize the working group's deliberations around two general questions: How are threat assessments prepared and used in practice? How might they be improved in execution?

Threat Assessment in Practice

What threats get emphasized -- bureaucratic and commercial incentives

Agency interests, sometimes supported by the engaged private sector, lead to emphasis on specific threats. For example, during the Cold War, the Air Force often overestimated the ballistic missile and bomber capabilities of the Soviets – and such assessments were used to justify military buildups in the U.S. Organizations tend to define problems in ways that relate to their mission; generally, they tend to focus on threats for which they can imagine an organizational response.

Organizational modes of operation, as well as political interests, play a role in determining which threats are considered seriously and which less so. For example, the U.S. and Russian nuclear commands continue to devote far more attention to deterring each other's deliberate nuclear strike than to addressing risks of inadvertent or accidental nuclear exchanges. Thus, both the U.S. and Russia still maintain each over 1000 nuclear warheads on high alert,

ready to be launched with tens of minutes of an order to do so. The U.S. nuclear command, while it can and does devote great attention to strengthening the U.S. command and control structure to assure that there cannot be a mistaken launch, cannot directly influence the Russian command and control structures. Taking the arsenals off of high alert would force the two sides' nuclear commands to develop new and unfamiliar operational procedures to address the possibility of a race to re-alert forces in a crisis.

Organizational and political interests help explain why the threat of terrorist attack was largely under-played before September 11th. It is striking that the Report of the U.S. Commission on National Security (the Hart-Rudman Report)—a thoughtful, bipartisan, and, in the event, prescient study pointing to the danger of terrorist attacks on the U.S. homeland—was not given prominence by the Clinton Administration and almost completely ignored by the incoming Bush Administration, Congress, and the media. At the time, there was no bureaucratic receptor for assessments of terrorism. Chris Preble, in his paper, explores several corollary reasons for the neglect of that assessment.

BOX 2: Threat Assessments Reviewed by the Working Group

Background paper

- (1) The 2001 U.S. Commission on National Security (“Hart-Rudman Commission”)*
- (2) The 2002 National Security Strategy (NSS)
- (3) The 2004 United Nations High-Level Panel on Threats, Challenges, and Change (“UN High Level Panel”)
- (4) The 2004 National Intelligence Council 2020 Project, Mapping the Global Future (“NIC report”)
- (5) The 2001 Quadrennial Defense Review (QDR)
- (6) The 2002 National Strategy for Homeland Security (NSHS)
- (7) The 2004 Report of the National Commission on Terrorist Attacks Upon the U.S. (“9/11 Commission”)
- (8) The 2004 National Commission on Energy Policy (“Hewlett Commission”)
- (9) The 2004 Carnegie Endowment for International Peace report, Universal Compliance: A Strategy for Nuclear Security (“Carnegie report”)

Preble paper

- (1) NSC 68: United States Objectives and Programs for National Security (1950)
- (2) The 1957 U.S. Congress, Joint Committee on Defense Production report, Deterrence and Survival in the Nuclear Age (“The Gaither Report”)
- (3) The 1976 NIE 11-3/8-76 (The “Team B Report”)
- (4) The 2004 National Commission on Terrorism (The “Bremer Commission”)
- (5) The 2003 Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (The “Gilmore Commission”)
- (6) The 2001 The United States Government Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN)
- (7) The 2001 U.S. Commission on National Security (“Hart-Rudman Commission”)*

* Reviewed both in Background and Preble papers.

Threat assessments are often affected by political considerations of various kinds. It has been pointed out many times, for example, that the initial decision to distribute homeland security funds largely across the states, rather than according to risk, did not correspond to any realistic assessment of which parts of the country were most at risk. This system of allocation is now changing with new leadership and information. However, more rational re-allocation of homeland-defense resources is stymied by the worry of politicians and officials that the public would hold them responsible in case of a successful attack on some sector where resources had been taken away.⁵

⁵ See James Fallows, “Success Without Victory,” *The Atlantic Monthly*, Jan/Feb 2005.

The reports that we reviewed identified many areas where the structure of incentives in government agencies and the private sector magnifies some threats while others do not get their full due. The 2005 Carnegie Endowment report, *Universal Compliance*, for instance, makes a compelling case for placing the highest priority on securing nuclear weapons and nuclear explosive materials in the former Soviet Union. Yet the report notes that the U.S. has devoted far more resources and urgency to addressing other, seemingly more remote threats, such as building a missile defense against a ballistic missile attack from a “rogue” country. The 2004 *National Commission on Energy Policy*, for example, has argued for a wide array of tax incentives, government spending, and other programs designed to realign commercial and bureaucratic incentives to favor technologies that could reduce the nation’s reliance upon imported fuels and polluting technologies. (These technologies include “coal gasification” that could allow the fuller use of the nation’s abundant coal resources and advanced nuclear power reactors, as well as more familiar initiatives to improve energy efficiency.) Recently signed comprehensive energy legislation adopted some similar fiscal incentives, and many firms and government agencies are now pursuing new energy technologies with greater vigor.

Overlooked threats

Threats without bureaucratic champions thus often get overlooked, but other factors play a role as well. One category of such threats are arguably those that involve events with low probability even when the outcome could be catastrophic, such as the one-in-ten-thousand risk of an asteroid of diameter greater than one kilometer hitting the Earth in the next century. It is not intrinsic to risks that are improbable but highly consequential that they are overlooked—witness, for example, the enormous investment in nuclear weapons deterrence during the Cold War.

In some cases, threats simply are not well imagined until some event focuses attention. We saw this recently in the change in threat assessments before and after 9/11 and after the anthrax attacks later that fall. Chris Preble points in his paper to instances where threat assessments during the Cold War did have considerable impact – most pointedly when they coincided or overlapped with some dramatic event.

As another illustration, the marked increase in attention to the threats of emerging diseases during the Clinton terms was in some measure due to a “bottom up” process, catalyzed by events such as the outbreaks of Ebola virus and the rise of other emerging diseases. An influential report from the Institute of Medicine of the U.S. National Academies was followed by a report by the Centers for Disease Control, and then an interagency report coordinated by the National Science and Technology Council. This was followed by the creation of an interagency group tasked with formulating a U.S. Government response strategy to the threat described in the earlier reports. The report of the interagency group, in turn, fed directly into a Presidential Decision Directive on the same topic, drafted by the individual who had chaired the interagency group. A subsequent study for the White House argued that the measures in the PDD should be built upon to improve the U.S. capabilities to respond to bioterrorism. In 1999, the Bioterrorism Preparedness and Response Program had been created within the CDC, and funded at \$118 million in FY 2000.

Events that dramatize one kind of threat could lead at the same time to the downplaying of others. Thus the threat of Al Qaeda, made palpable on 9/11, may deflect attention away from threats posed by domestic terrorists. The attention to Al Qaeda has led all Islamic terrorism to become grouped under a single heading when there may be quite large differences in intentions and capabilities.

Finally, some threats may be ignored or downplayed simply because the assessments are mistaken. For example, Bunn and Wier point out that the belief – mistaken in their view – of many analysts in the U.S. that a terrorist group could never put together a nuclear device without significant help from a state sponsor has contributed to a lack of urgency in securing nuclear material in Russia and elsewhere: “It is this myth – the supposed need of state sponsorship – that above all others has led many of the most senior officials of the U.S. government to place only modest priority on securing the world’s stockpiles of nuclear weapons and materials.”⁶

Unintended Consequences of Threat Assessments

It is possible that threat assessments can have unintended (and undesirable) consequences. This possibility may be seen in the ongoing biological threat assessments now underway in the U.S. Such is argued by Jonathan Tucker in a recent article, “Biological Threat Assessment: Is the Cure Worse than the Disease?”⁷ Without necessarily endorsing Tucker’s specific conclusions, we may use his analysis to provide an illustration of the role of unintended consequences.⁸

Tucker argues that a key component of the threat assessments now being done is the development of pathogens engineered to be resistant to multiple antibiotics. Such work is needed, the Administration claims, to shorten the time between the discovery of new bioterrorist threats and the development of medical countermeasures, such as vaccines and therapeutic drugs. Tucker argues the flaws and dangers of this argument. First, this biodefense agenda credits terrorists with having technological capabilities they are not likely to possess or acquire. (The Soviet Union did develop such capabilities, but such capabilities, he argues, are far from terror groups.) Second, the creation of hypothetical pathogens is of limited value because of the difficulty of predicting technological innovations by prospective enemies. And third, such work blurs the hazy line between offensive and defensive biological development, and will raise suspicions around the world about the compliance of the U.S. with the Biological Weapons Convention (BWC), which forbids the development of offensive bio-weapons but is silent on the research that could lead to such weapons. The U.S. threat assessment activities therefore run the risk of inadvertently creating pathogens which could eventually be appropriated by real enemies,

⁶ Matthew Bunn and Anthony Wier, “The Seven Myths of Nuclear Terrorism,” *Current History*, April 2005.

⁷ Jonathan Tucker, “Biological Threat Assessment: Is the Cure Worse than the Disease?,” *Arms Control Today*, October 2004.

⁸ Chyba presented his own analysis of some of these issues in Christopher F. Chyba and Alex L. Greninger, “Biotechnology and Bioterrorism: An Unprecedented World,” *Survival* vol. 46, no. 2, Summer 2004, 143-162.

of giving rise to a large number of “insiders” with knowledge how to make the pathogens, and of provoking an arms race with other countries suspicious of the U.S.

A study underway at Los Alamos National Laboratory, which has recently come to light, raises similar concerns. In this study, reported in the *Washington Post* in July 2005, researchers are constructing elaborate computer models that include information on all the known vulnerabilities of the U.S. There are virtual power grids, transportation systems, oil and gas lines, and the like. “If the simulations got into the wrong hands, the researchers say, they could be used as the ultimate weapons against Americans.”⁹ Again, this is not to say that such studies should not be done, but to point to the dangers inherent in certain kinds of threat assessments.

The Private Sector

It is critical to recognize that a growing array of threats to national security has, increasingly, required the engagement of the private sector. This is especially so with homeland security, where the country must address threats to air transportation, chemical plants, the electric grid, nuclear power plants, oil refineries, and other industries.

For such threats, there are three immediate implications. First, and most obviously, the knowledge and capabilities to understand and respond to the threats do not reside solely or even mainly with government. On the contrary, they may well reside predominantly with private enterprise and individuals outside of government. In some areas, such as the launching of computer viruses and other cyber threats, government may have an especially difficult time staying abreast of the dangers because the frontier of knowledge moves quickly, most resources are mobilized outside government, and the most entrepreneurial experts tend to be privately employed.

Second, the means to address the threats identified will often involve large costs which the private actors may be reluctant to expend. It will not be surprising to see such private actors – say in the aircraft or chemical industry – opposing stringent new measures of protection. Moreover, since in many of these industries, there exist multiple pathways by which terrorists could strike, there will be an added reluctance by the industries to devote resources to closing off any one pathway. We describe one illustration of this dilemma in the accompanying box on the threat to airplanes from shoulder-fired missiles (see Box 3).

⁹ Ariana Eunjung Cha, “Computers Simulate Terrorism’s Extremes,” *Washington Post*, July 4, 2005.

BOX 3 – Shoulder-Fired Missiles

The threat to commercial aircraft of shoulder-fired missiles provides a good illustration of the dilemmas of threat assessments relevant to homeland security and the interplay of private and public interests. The illustration here is based on the study by Charles Pena of the Cato Institute [Charles V. Pena, “Flying the Unfriendly Skies: Defending against the threat of Shoulder-fired Missiles,” *Policy Analysis*, Cato Institute, April 19, 2005.]

Shoulder-fired anti-aircraft missiles – man-portable air defense systems (MANPADS) – pose a threat. They have proliferated around the world and they have the capability to strike at commercial aircraft. If one such missile was successful in downing an aircraft, the event could cripple the air industry and lead to economic losses in the several tens of billions of dollars.

Let us stipulate that it is possible to defend against this threat, by placing on all U.S. commercial aircraft advanced laser-jamming infrared systems. The cost of doing so would be around \$11 billion plus \$2 billion per year in recurring costs. Should this be done?

Pena at Cato argues it should be. The cost-benefit calculus supports doing so. But others oppose this. For example, the RAND corporation concluded that any decision to emplace countermeasures on aircraft should be put off for the time being for several reasons: annual operating costs would be half of what the federal government currently spends for all transportation security in the U.S.; terrorists will likely be able to devise attack scenarios that could defeat countermeasures; and installing countermeasures could simply divert terrorist efforts to less-protected opportunities for attack. The Air Lines Pilots Association also has not embraced installation of the countermeasures, especially if the industry has to bear the costs.

The arguments on both sides are weighty, with the dilemma strikingly captured by Pena: “So a realistic approach to homeland security starts with understanding that a perfect defense against terrorism is not possible. It also means knowing that even if defenses are erected, the nature of terrorism is to morph and adapt, to flow around obstacles, and to find the least resistance. Therefore a determined enemy will eventually find a way to exploit gaps in defenses and security – precisely what Al Qaeda did on 9/11.” Is it reasonable, in this view, to devote substantial resources to addressing one pathway to attack when the enemy could over time find other pathways “to flow around obstacles?” As noted, the RAND analysts did not think so. Pena, despite his understanding of the ability of the enemy to pick its point of attack, thought otherwise.

Third, the methods for analyzing threats and the metrics for success tend to differ systematically between the private and public spheres. In the public sphere, the security apparatus tends to frame its problem as one of “threat assessment.” Once a threat has been identified, the security paradigm tends to assume that a response is required. By contrast, in the private sector most such issues are examined through a framework of risk management—priorities are set on risks, responses merit investment only to a point, and certain levels of loss (and risks of loss) are tolerable. In risk analysis, there is an often explicit cost-benefit approach to a problem, whereas governmental threat assessments rarely refer, explicitly at least, to cost-benefit considerations. Often, such risk assessment is performed with quantitative methods and subjected to rigorous updating with new information.

This difference in approach may be best revealed in the electric power sector. With growing concern with vulnerabilities in the electric grid, the Government has increased pressure on operators to invest in additional guards, gates and guns—to harden the infrastructure. While the utilities and groups managing the grid do not by any means oppose such hardening, they put equal or more attention to investments in redundancy, flexibility, and capability for rapid responses to unexpected shutdowns of parts of the overall system. They naturally seek a very high standard of reliability, but at the same time continually weight the costs of outages against the cost of ensuring additional system resilience.

In general, the central role of private sector actors in threat assessment and mitigation will require many different kinds of initiatives, some of which have already been taken. For example, it will be necessary for the government to grant security clearances to key personnel in the private sector, to relax certain anti-trust and freedom-of-information regulations so as to allow entities within a sector (say, the electricity sector) to compare notes and exchange data, and to arrange rapid communication channels between the private sector and government security agencies.

The degree to which private sectors will be able to undertake sector-wide threat assessments and actions will vary widely. In the electric power sector, for example, such coordination of action is made possible through the North American Reliability Council (NERC) by the relatively limited number of actors involved. NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to assure the reliability of the electric grid. It coordinates ten regional reliability councils representing all segments of the electric industry – private utilities, rural cooperatives, independent power producers, and others; and it has established a remarkable degree of independence in recognizing threats to the grid and to responding to such threats. It has, for instance, undertaken planning, training, and operating program to prepare for various natural disasters such as earthquakes, floods, tornados, energy emergencies, and attacks of sabotage and terrorism; and it has developed close working relations with government security agencies.¹⁰ (The new comprehensive energy legislation, finalized in August 2005, will shift NERC’s operations to a new organization and make NERC’s reliability standards legally binding.)

¹⁰ Michehl Gent, “Securing Our Infrastructure: Private/Public Information Sharing,” *Hearing Before the U.S. Senate Committee on Governmental Affairs*, May 8, 2002.

Comprehensive sector-wide assessment does not appear possible, by contrast, in the realm of cyber security where there are millions of actors.¹¹ According to Ed Felten, Professor of Computer Science at Princeton, and member of our working group, the roots of vulnerability here are in the intrinsic bugginess of software, and in limitations in defense mechanisms such as checking and scanning and walling off a computer system. Bugs are important because attackers break in by exploiting bugs; and they are probably unavoidable. Felten estimates that at present in industrial-quality codes there is one serious bug per 10,000 lines of code. Windows, which has 40 million lines of code, by this count would contain 4,000 serious bugs. An attacker could use the bugs for either targeted attacks or viral attacks.

In a targeted attack, the hacker aims at a specific target for a specific purpose. In general, this kind of attack requires high technical skill, intelligence about the target, and possibly insider information. Protection will be the task of computer experts at the individual potential targets.

A viral attack spreads on its own, and potentially widely. It requires a propagation mechanism and a payload (what damage or message is conveyed to a computer). A fast viral attack, in a realistic worst case, could infect the whole internet in ten minutes! A viral attack could also be slow and stealthy, installing “bots” on each compromised machine, ready to be unleashed at some later time at some command. Protection against viral attacks of both kinds is provided in part by an army of computer experts around the world, working rapidly when a new virus is discovered. As with targeted attacks, there are too many actors and too many machines and vulnerabilities for one to imagine some central coordinating agency such as NERC.

Improving Assessment Methods

Avoiding Groupthink

Several recent studies of the failure of U.S. intelligence with respect to weapons of mass destruction in Iraq have pointed to a kind of group-think that made it difficult for analysts to consider contrary views to the prevailing conventional wisdom and assumptions.¹² Our group did not examine the questions surrounding these weapons; rather, we looked further back in history where the lessons are easier to identify. We find that group-think is less evident in the threat assessments we have looked at, but it probably exists to some degree. One possible illustration is the way many U.S. analysts think about terrorists. Before the terrorist incidents of the 1990’s and culminating in the September 11 attacks, there was a wide consensus that

¹¹ This discussion is based on the presentation to our working group by Ed Felten, “Cyber-Attacks,” Stanford, April 4, 2005.

¹² For example, in the Silberman/Robb review of intelligence before the Iraq invasion concluded: “The failure was in large part the result of analytical shortcomings: intelligence analysts were too wedded in their assumptions about Saddam’s intentions.” Lord Butler’s report noted that “care should be taken to ensure that worst case analysis is not carried forward into assessments except those (like assessments of enemy capabilities) which warrant such an approach.” Pervasive in both these reports is the hypothesis that a particular set of conclusions had permeated the organizations that were providing intelligence estimates to national security decision-makers.

terrorists wanted to make a political point and that this was far more important to them than causing casualties. In the aftermath of 9/11, the consensus has swung to the opposite extreme – that terrorist groups are determined to cause as many casualties as they can. However, this may not be true for all terrorist groups, and the question of when it is and is not must be asked.

Two ideas discussed by our working group to combat group-think were: the more systematic use by those developing national security policy of the National Intelligence Council (NIC) and Intelligence and Research (INR) in the State Department; and of Solarium or Team B exercises. NIC and INR appear especially well positioned to offer critiques of threat assessments done by groups elsewhere in the government—both organizations lack a specific policy responsibility and mission yet have considerable expertise in virtually all regions of interest to the U.S.

Chris Preble, as well as Michèle Flournoy and Shawn Brimley, discuss the use of the Solarium group in the Eisenhower Administration to illustrate one strategy for avoiding groupthink. In the summer of 1953, Eisenhower directed his national security staff to undertake a unique project to test competing strategies for addressing the Soviet threat. Project Solarium, so named because it was first conceived in the White House solarium, involved teams of national security experts, each tasked with making a case for one of three distinct strategies. One task force was to advocate an aggressive rollback strategy. A second was responsible for articulating a classic containment strategy (this task force chaired by George Kennan), a third task force called for containing Soviet aggression through deterrence, but one, unlike Kennan-style containment, which would be exercised “less timidly and more unilaterally.” A crucial component of this more aggressive containment strategy would be the threat of general war to deter the Soviets.¹³ Each task force was to justify the threat assessments that underlay the strategy being advocated; and each was to explore the full range of implications of its strategy. In the event, the project appears to have been successful in sharpening Eisenhower’s strategic synthesis, which at the end contained elements of the containment and the aggressive containment views.

Intentions and Capabilities

We have found that most assessments have emphasized the capabilities of potential enemies, without much sustained attention to their motives. For example, the 2002 U.S. National Security Strategy devoted almost no analysis to the motivations of terrorists, “rogue states,” and other adversaries. Such excessive attention to capabilities may reflect that they often can be gauged more objectively than can motives and worldviews.

It is striking that George Kennan’s X article and long telegram, which are often invoked as models for a new national security overview, were almost entirely devoted to an analysis of the beliefs and behavior of Soviet leaders. To Kennan, capabilities, while important, were of secondary concern. In an article in *The Atlantic Monthly*, James Fallows (a member of our

¹³ An excellent source on the Solarium Project, and on the formulation of Eisenhower’s national security strategy more generally, is Bowie and Immerman, *Waging Peace*, especially pp. 123-138. See also Gaddis, *Strategies of Containment*, 145-146.

working group), emphasized this point: “No principle of warfare is more familiar than the maxim ‘Know your enemy.’ No concept has been more thoroughly ignored by the United States in its efforts to eliminate the root causes of Islamic terrorism since 9/11.”¹⁴ In the words of Ambassador Robert Hutchings (also a member of our group), applying Kennan’s strategic logic to the problem of terrorism requires going “beyond the symptoms of the problem to address its underlying causes.”¹⁵

It can be difficult to identify accurately the intentions of adversaries. Some Cold War assessments of the mindsets that animated Soviet leadership seem, in retrospect, highly tortured. For example, tracts were written on why the Soviets believed they could fight and win a nuclear war. In the 1980s, the idea of a window of vulnerability was put forward by the Committee on the Present Danger (CPD) and embraced to a point by the defense establishment. The so-called window was thus: The Soviets in a first strike could destroy all the U.S. land-based missiles. Our sea-based missiles would survive but they could not be used since we would be deterred – that is, the Soviets would say that if we used the missiles in retaliation, the Soviets would respond by striking U.S. cities. Another related line of argument was that Soviet leaders would not be deterred by threat of destruction of their cities. What they really cared about is their power and control of the country – and so the threat of millions of casualties would not in itself deter them.¹⁶

A focus on capabilities at the expense of intentions in war planning was also allied frequently with the adoption of “worst-case” reasoning. In early 1976, the new CIA director, George Bush, appointed a group of private citizens to take an independent look at the Soviet threat – independent, that is, of the CIA official analysis (“Team A”) which some observers believed insufficiently concerned. The group – Team B -- tended to the “hawkish” view, and it was chaired by Richard Pipes, known for fierce anti-Soviet views. And, in the event, on every substantive point, Team B stressed and enlarged the perception of danger and a threat. The widest differences between the Team A and Team B assessments pertained to Soviet intentions and motives, where there was enormous opportunity for subjective interpretation and highly intuitive judgment.

While the Team B analysis seems in retrospect to have provided an exaggerated view of the Soviet threat, the idea of “competitive analysis” embedded in the Team B approach does not seem unreasonable. Preble quotes Raymond Garthoff on this. The notion of “outside experts offering some alternatives to test was not without merit,” still “the terms of reference should have been clear, and there should have been two alternative teams and viewpoints, one more pessimistic but the other more optimistic.... It is clear in retrospect, that what had been needed in 1976 was not a hard-line Team B, but a more imaginative and far-seeing ‘Team C.’”

Quantitative Methods and Social Science

¹⁴ James Fallows, “Success Without Victory,” *The Atlantic Monthly*, Jan/Feb 2005.

¹⁵ Robert L. Hutchings, “X + 9/11” *Foreign Policy*, July/August 2004.

¹⁶ The role of the CPD is discussed more fully in the Chris Preble paper.

It is intriguing to us that a large and growing body of social science research appears not to have been much tapped to inform assessments. Such research includes, for example, studies on the causes of war and civil conflict, suicide terrorism, the links (or not) between poverty and terrorism, the difficulties of deterring non-state actors, and other topics.¹⁷ While we did not perform a systematic analysis of the social science bases of each threat assessment that the group discussed, the connections between such research and the practice of threat assessment appears to be weak.

We also wonder whether threat assessments could make fuller use of scientific methods. In this thinking, we benefited from a briefing by Elisabeth Paté-Cornell at our Stanford meeting. Our discussions identified three ideas worth pursuing further.

First, we believe it would be helpful if intelligence findings within threat assessments indicated on some scale the degree of confidence that the authors have in their sources, and in their findings. None of the threat assessments that we examined included systematic attention to probabilities or even a more general level of confidence in their conclusions.¹⁸

Second, a more ambitious initiative, as suggested by Paté-Cornell, is to make more systematic use of Bayesian analysis coupled with systems analysis.¹⁹ Using such analyses, analysts or policy makers will first continually revise their representation of the structure of a threat and the possible scenarios of attacks. They will also continually update their probability estimate of some event or fact in light of new evidence. In other words, prior judgments are exposed in a rigorous way to confirming or contradictory intelligence. Bayesian analysis simulates how most people think about complex systems, but it allows a more rigorous assessment of complex systems, including the assessment of probabilities of certain outcomes.²⁰

Third, we are struck that the new generation of threats—such as emerging diseases, global economic contagions, and climate change—will require the involvement of scientific assessments that traditionally have been largely outside the practice of traditional threat assessment. In addition to building the capacity to perform such analyses within the normal mechanisms for threat assessment in government, these challenges might be met with some organizational reforms. Government might profitably make fuller use of the National Academy

¹⁷ For example, Robert Pape, “The Strategic Logic of Suicide Terrorism,” *American Political Science Review*, Vol. 97, No. 3, August 2003; Scott Atran, “Genesis of Suicide Terrorism,” *Science*, Vol. 299, 7 March 2003.

¹⁸ Michael Schrage, “What Percent is ‘Slam Dunk’? Give Us Odds on Those Estimates,” *Washington Post*, February 20, 2005.

¹⁹ This analytical approach involves creating a detailed quantitative description of the system that is at risk and then assessing the risks and consequences of different types of attacks; as new information is gathered, those risk assessments are updated. Such an approach has the merit of being transparent in its assessment of vulnerabilities and consequences; it also allows an assessment of the value of different types of information, which can help to improve intelligence gathering.

²⁰ See Elisabeth Paté-Cornell, “Fusion of Intelligence Information: a Bayesian Approach,” *Risk Analysis*, Vol. 22, No. 3, 2002; “Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures,” *Military Operations Research*, Vol. 7, No. 4, 2002; Bruce Blair, “The Logic of Intelligence Failure,” Center for Defense Information, March 9, 2004, at www.cdi.org.

of Sciences complex—evident, already, in areas where NAS is active such as emerging diseases and climate change. In addition, such assessments will tax the government’s ability to manage inter-agency coordination since most of the government’s talent for such assessments is scattered across the bureaucracy.

Threat Assessment as a Means of Organizational Management

Threat assessments appear to serve at least two purposes. One, most obviously, is to inform the setting of national security priorities, including the allocation of resources. A second purpose may be less well understood yet vitally important: socialization. The Quadrennial Defense Review (QDR) threat assessments for example have served to align review participants around a common vision. They allowed a disparate group of analysts and officers inside the Pentagon to ponder threats and responses together – but by the same token, the process did understandably focus largely on military responses to gathering threats.

To the extent that threat assessment plays this role, it may be possible to recast the process of assessment so that it aids in managing the disparate organizations that must align around a common vision if the U.S. is to develop and implement an integrated national security strategy.

Using the QDR and some historical examples of strategic planning by the National Security Council as a starting point, Michèle Flournoy has explored the prospects for an expanded QDR-like process that would engage agencies and departments other than Defense, which might be termed a quadrennial national security review (QNSR). Previous administrations have attempted to undertake strategic planning for national security with mixed success. The Bush Administration did publish in 2002 a National Security Strategy, but this was mainly an articulation of national goals and objectives for the public and Congress. It did not involve the high-level attention and careful staff work that characterize the QDR. Nor did it provide authoritative guidance for internal stakeholders on how to manage risk and allocate resources. So what is needed, Flournoy argues, is a serious multi-agency assessment and strategic planning process for national security. Such an approach would help to overcome the stove-piping of assessments—especially between the intelligence community, the Pentagon, and State—and could make it easier to connect actual bureaucratic practice to underlying threat assessments. A quadrennial national security review will face several obstacles, but if these were overcome, could have significant value.

We note that there are some incomplete precedents for this type of review; for example, the interagency process that led to the Clinton Administration’s PDD on the government response to emerging diseases produced a strategy that required consensus and then coordinated actions among the Department of State and Defense, the Centers for Disease Control and the National Institutes of Health, USAID, and the National Security Council and White House Office of Science and Technology Policy.

Conclusions

Our deliberations, along with the background papers, have led us to the following conclusions.

First, most recent threat assessments have focused on the capabilities of enemies and vulnerabilities in U.S. defenses, but have been notably weak in assessing the enemies' intentions – their worldview, motives, modus operandi, strengths and weaknesses. This is especially surprising in that the Kennan X article and long telegram, often invoked as models of threat assessment and national security strategy, focused almost entirely on an analysis of Soviet intentions, beliefs, and behavior. This finding is sobering as we enter a new era with new enemies whose intentions have proved particularly difficult to assess.

Second, the national security apparatus should be alert to unintended consequences of threat assessments. One sobering illustration is in the area of biodefense. A key component of the threat assessments now being done in this realm is reportedly the development of pathogens engineered to be resistant to multiple antibiotics. Such work may be needed, but we should also be aware that there are dangers -- of creating pathogens which might eventually be appropriated by bad actors, which would give rise to a large number of "insiders" with knowledge how to make the pathogens, and of provoking an arms race with other countries suspicious of the U.S.

Third, we are struck that a growing array of threats to national security requires the engagement of the private sector. The knowledge necessary for assessment and the capabilities for response lay, in these cases, with private enterprise and individuals largely outside the employ of government. Many of the security issues with these attributes relate to homeland security, such as air traffic, chemical plants and oil refineries, the electric grid, and computer infrastructures.

Fourth, properly assessing many of the new threats to national security—such as emerging diseases, global economic contagions, and climate change—will require the involvement of experts from disciplines outside the traditional practice of threat assessment. Much of the expertise needed for such assessments already exists, but tapping it will require efficient mechanisms for working across government agencies and for engaging the scientific community beyond government.

Fifth, we are impressed by the wide array of organizational and analytical reforms that could improve the practice and utility of threat assessment. These include:

- Although it went beyond just threat assessment, the Solarium technique used by President Eisenhower in 1953 is worthy of attention; possibly the technique could usefully be emulated by those constructing U.S. grand strategy today. In the Solarium project, the President set up three teams, each charged with developing and arguing for a particular strategy: one team was to examine "roll-back." A second was to focus on "containment" -- this team chaired by Kennan. A third team

looked at what might be called "aggressive containment" -- a containment strategy exercised "less timidly and more unilaterally."

- We believe that there could be more productive use of quantitative measures in threat assessments, such as Bayesian analysis. In addition, there is an urgent need for assessments to include fuller information about the levels of confidence and probabilities of outcomes. Most key conclusions in such assessments require judgments that are far from certain, but often the reports do not include sufficient information to allow users to ascertain the analysts' confidence in their conclusions.
- There appears potential value in the government undertaking what might be called a quadrennial national security review (QNSR), which would complement the QDR. The National Security Strategy published by the Administration provides a useful overview of current Administration thinking, but unlike the QDR it did not appear to engage the high-level attention and task force work which underlies the QDR. A QNSR could help to overcome the stove-piping of assessments-especially among the intelligence community, the Pentagon, and State -- and could make it easier to connect actual bureaucratic practice to underlying threat assessments. A serious quadrennial national security review will face several obstacles, but if these were overcome, could have significant value.