



**REPORT OF THE WORKING GROUP ON RELATIVE THREAT ASSESSMENT
CO-CHAIRS: CHRISTOPHER CHYBA, HAL FEIVESON & DAVID VICTOR**

Executive Summary

The United States faces three classes of threats: 1) those where there is an identifiable enemy agent, such as a government or terrorist group; 2) those that derive entirely or in part from human action but not from hostile intent, such as climate change, accidental nuclear war, or emerging diseases; and 3) those that stem from natural disasters such as earthquakes or asteroid impacts.

Threat assessment in practice

Most threat assessments have focused on the first class of threats—those originating from a hostile enemy. These assessments have tended to overemphasize enemy capabilities without much sustained attention to enemy motives or intentions. The best threat assessments connect instead three principal foci of analysis—enemy capabilities, enemy intentions, and U.S. vulnerabilities—to provide a full picture of the origins and consequences of actions that threaten U.S. interests. Such assessments can then be used effectively to set priorities for national security strategy and budgets.

In practice, bureaucratic and commercial incentives have a strong influence on the threats that are considered and treated seriously by the United States. These incentives include agency interests, organizational modes of operation, and political pressures. The structure of incentives in government agencies and the private sector frequently magnifies some threats while overlooking others; thus, threats without bureaucratic or private sector champions are often overlooked.

Other factors influence government responses to threat assessments as well. The government sometimes overlooks: threats involving very low probability events even when the outcome would be catastrophic; poorly imagined threats, such as the possibility before 9/11 of using airplanes as bombs; and threats overshadowed by other, more salient threats.

Threat assessments can have unidentified (and undesirable) consequences. This possibility is illustrated by the ongoing biological assessments underway in the United States, the consequences of which run the gamut from the risk of inadvertently creating pathogens that could eventually be appropriated by real enemies, to the rise of a large number of “insiders” with knowledge of how to make the pathogens, to an arms race with other countries suspicious of the United States.

A growing number of national security threats require the engagement of the private sector, especially in the realm of homeland security, and have three immediate implications. First, the knowledge and capabilities needed to understand and respond to the threats do not reside solely or even mainly with the government. Second, the means to address the threats often involve large costs that private actors may be reluctant to expend. Third, the methods for analyzing threats and the metrics for success tend to differ systematically between the private and public spheres. To strengthen public-private cooperation in threat assessment and mitigation, the government should grant security clearances to key personnel in the private sector, relax certain anti-trust and freedom-of-information regulations, and establish rapid communication channels between corporations and government security agencies.

Improving assessment methods

A proper assessment of many new threats requires the involvement of experts from disciplines and institutions that are outside the traditional practice of threat assessment. To tap this expertise, the United States needs efficient mechanisms for promoting collaboration across government agencies and engaging, beyond government, the scientific and business communities. By conducting a quadrennial national security review, in which all agencies involved in national security would perform assessment and strategic planning jointly, the government could take an important step toward overcoming the bureaucratic stove-piping of assessments. At the same time, it could engage scientists outside government more effectively through institutions such as the National Academy of Sciences.

Threat assessments must be organized to avoid the perils of groupthink. Analytical exercises modeled after President Eisenhower's Project Solarium, which tasked teams of experts to advocate for alternative national security strategies, can help ensure that assessments consider competing perspectives. Assessments should also make fuller use of social scientific methods and should include assessments of confidence in findings, with outlier opinions as well as more likely estimates.