RAND CORPORATION

TESTIMONY

CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

## Support RAND

Browse Books & Publications

Make a charitable contribution

## For More Information

Visit RAND at www.rand.org

Explore RAND Testimony

View document details

### Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.

TESTIMONY

# Emerging Threats to National Security

GREGORY F. TREVERTON

CT-234

February 2005

Testimony presented to the House of Representatives Permanent Select Committee on Intelligence on February 2, 2005

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
RAND® is a registered trademark.

Published 2005 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

**Statement of Gregory F. Treverton**[1]
**Director, Intelligence Policy Center**
**The RAND Corporation**
**Associate Dean, Pardee RAND Graduate School**

**Before the Permanent Select Committee on Intelligence**
**United States House of Representatives**

**February 2, 2005**

Chairman Hoekstra, and other members of the Committee, thank you for inviting me to testify today on future threats with which the U.S. Intelligence Community will have to deal. It is a pleasure to be here. The Intelligence Reform and Terrorism Prevention Act of 2004 made an important start in reshaping U.S. intelligence, but in many respects the harder part – reshaping the cultures of organizations, in addition to the organization charts – lies ahead of us. And there is no better place to start than at the beginning, with the threat.

My comments today are informed by a number of recent RAND Corporation projects I have done, in addition to my previous stints of service in government. In particular, I had the opportunity to think about how the change in intelligence's targets – from state targets to transnational ones, like terrorism – dramatically changed the way intelligence needed to go about its business. That work has been done for the CIA's Sherman Kent Center for Analytic Tradecraft, for the Assistant Director of Central Intelligence for Analysis and Production (ADI, A&P), and for the Information Technology Innovation Center (ITIC).[2] The framework I use today – moving from broad global drivers, to effects bearing on U.S. national security, to implications for U.S. intelligence – grew out of

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] The papers from the Kent Center project are Treverton and Warren Fishbein, *Making Sense of Transnational Threats*, Central Intelligence Agency, Kent Center for Analytic Tradecraft, Occasional Papers, 3, 1 (October 2004), www.cia.gov/cia/publications/Kent_Papers/pdf/OPV3No1.pdf; Abbreviated version published separately as "Rethinking 'Alternative Analysis' to Address Transnational Threats," Kent Center for Analytic Tradecraft, Occasional Papers, 3, 2 (October 2004), www.cia.gov/cia/publications/Kent_Papers/vol3no2.htm

work RAND has done for the Federal Bureau of Investigation on threat forecasting and strategic planning, and more recently, a project being done for AS&T at the National Reconnaissance Office (NRO). That framework has seemed useful for a variety of intelligence agencies in positioning themselves for a very different future.

The starting point for thinking about the intelligence requirements of 2020 – for the Intelligence Community as a whole or for particular agencies – is with what will drive that future. The drivers are tolerably clear even if exactly how they will play out is not. Those drivers are interconnected but can be grouped in nine clusters.[3]

- Communications revolution
- Economic globalization
- Other technological revolutions
- Revolution in military affairs
- Identity politics – "us" versus "them"
- Global demographics
- Environmental concerns
- Role of state and law
- U.S. foreign policy

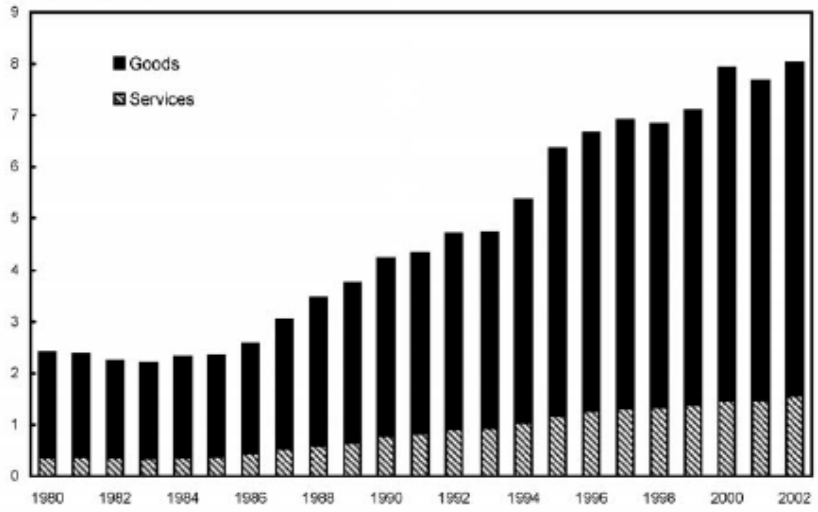
**GLOBAL DRIVERS**

*Communications revolution:* The information revolution is a key enabler of economic globalization. It was the information revolution that undid the Soviet Union, for while planning and brute force could produce roads and dams, they could not induce innovation in computer chips. However, communications also makes it possible, for instance, for terrorists and drug traffickers to encrypt their communications, or for would-be Haitian boat people to learn within a day what fraction of their predecessors have been screened into the United States.

*Economic globalization:* The international economy will continue to be characterized by opening markets, virtually unrestricted capital flows, and the global reach of multinational firms. "Bads" – arms, drugs,

[3]See Treverton, *Reshaping National Intelligence for an Age of Information,* (Cambridge: Cambridge University Press, 2001), chapter 2. Not surprisingly, given that the world is the world, other efforts to frame the future begin with similar sets of drivers. See UK Ministry of Defence, Joint Doctrine and Concept Centre (JDCC), *Strategic Trends,* (www.jdcc-strategictrends.org/index.asp); National Intelligence Council, *Global Trends 2015: A Dialogue about the Future with Nongovernment Experts (*www.odci.gov/nic/pubs/index.htm); Center for Strategic and International Studies, *Seven Revolutions Project;* National Imagery and Mapping Agency, *Understanding Global Change*.

lethal materials or weapons, and laundered money – will move almost as freely across borders as goods like trade, investment, financial flows, and technologies. However, the global economy is driving the haves and the have-nots further apart, including in the United States, and the backlash against globalization may pose a specific threat to America's security when activities turn to riots and violence to protest multinational corporate power.




SOURCE: U.S. Council of Economic Advisers

**Fig. 1–World Trade in Goods and Services, 1980-2002**

*Other technological advances:* The communications and information revolutions will be joined by rapid advances in biotechnology, biometrics, microelectronics, nanotechnology, and materials technologies. Progress in the range of wired and wireless technologies will make for faster and cheaper flows of information around the world. These technologies will also permit information to be stored and processed in new ways. For instance, Internet Voice, also known as Voice over Internet Protocol (VoIP), allows individuals to make telephone calls using a broadband Internet connection instead of an analog phone line. The life cycles of both products and processes will be shorter and shorter, and their diffusion around the world quicker and quicker, making it difficult for intelligence to keep up with innovations. New technologies can improve the ability to perform genetic and blood analyses; monitor and track adversaries; and gather information. At the same time, however, those same technologies will make it easier for terrorists, criminals, and spies to communicate with each other, distribute propaganda, gather information, conduct

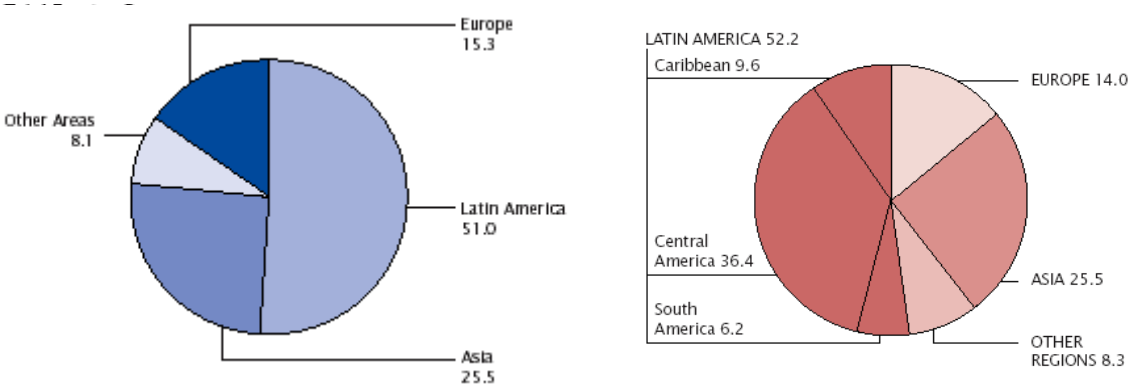
espionage, and criminal activity, and target the U.S. through cyber attacks.

*Revolution in military affairs*: What has been termed a "revolution in military affairs" will continue, driven by improvements in computers and electronics. Sensors are becoming radically more capable, making the future battlefield "transparent." Land vehicles, ships, missiles, and aircraft may become drastically lighter, more fuel efficient, faster, and more stealthy, making U.S. forces more rapidly deployable. Advanced munitions will make them more lethal once deployed. New types of weaponry – such as space weapons, directed energy beams, and advanced biological agents – may be developed. However, there has been less "revolution" in policing and contingency operations that still require – and endanger – large numbers of soldiers.

*Identity ("them" vs. "us") politics:* People's tendency to seek identification with "us" and to distinguish "us" from "them" seems on the rise everywhere, perhaps inside the United States as well. This is perhaps partly in reaction to globalization, which can be dizzying in its pace, destructive to cultural icons, and pushed by forces beyond anyone's control. The distinguishing factor may be religion, or ethnicity, or neighborhood (or even family). The most visible manifestations will be a rise in Islamic extremism in the Middle East, Asia, and Africa, along with an increase in transnational organized crime based on ethnicity and familial ties. Ideological revolutions in such countries as Saudi Arabia or Pakistan could bring to power regimes hostile to the United States. America's military, cultural, and economic pre-eminence will continue to make it the target of violence unleashed for ideological and religious reasons. Finally, a rise in legal or illegal immigration may eventually lead to xenophobic cults and militias at home, with the capabilities and desire to attack immigrants.

*Global demographics:* Almost all the global population growth will continue to occur outside the current industrialized countries, and some rich countries (and others, like Russia or South Africa) may actually decline in population. The United States will continue to grow, but two-thirds of that growth will be legal and illegal immigrants, mostly from Latin America and Asia. Furthermore, there will likely be a continuing rise in urbanization as immigrant populations move to such metropolitan areas as New York, Los Angeles, and Chicago. Global demographic changes could also impact America's threat environment, creating "youth bulges" of unemployed young men in the Middle East, Asia, and Africa.

2000 2002




Source: U.S. Census Bureau

**Fig. 2-Immigration to the United States By Source (in percent)**

*Role of state and law:* This driver encompasses two broad changes. First, while the nation-state is not about to go away, it will increasingly have more competitors, ranging from corporations and non-governmental organizations (NGOs) to terrorists and criminals. For example, terrorist organizations may receive less state sponsorship and become more difficult to monitor and deter. Second, international law is changing from its preoccupation with states to a consideration of individuals as fit subjects. In one sense, the represents movement of international law in an "American" direction, that is toward the primacy of the individual. At the same time, it may put U.S. citizens at risk of international scrutiny and inhibit states' abilities to do as they choose with their own citizens within their borders.

*U.S. foreign policy:* Because the United States is and will remain such a dominant power, its own actions will be a key driver of the future. Just as conventional U.S. military might compels potential adversaries to attack it asymmetrically, so, too, tactical successes, like that against Al Qaeda, cause those asymmetric threats to morph into less hierarchical, more fragmented – but perhaps still dangerous – forms. More generally, U.S. actions and policies on a range of issues from Iraq, Saudi Arabia, Pakistan, and Syria, to the Israeli-Palestinian peace process, will affect America's future threat environment. They may do so directly, by requiring continuing deployments of American

power, or less directly, by animating anti-U.S. anger and so providing fertile ground for terrorist recruiters.

**From States to Transnational Targets**

In many respects, the biggest question raised by pursuing the drivers through their effects to their implications for intelligence is: what is intelligence? When there was one over-arching target, the Soviet Union, that was secretive, and a small number of consumers, the answer seemed clear. Intelligence was finding out those things that would-be adversaries did *not* want us to know. Many of those were *puzzles,* questions that had definitive answers if only we had the information: how accurate were Soviet rockets, for instance?

Now, the answer is less clear. Many of the questions for intelligence are *mysteries,* future and contingent, questions whose answers would-be adversaries may not want us to know but answers that they themselves do not know either. While some of those foes are secretive, there are torrents of relevant information that is not secret – ranging from motor vehicle records to posting on the Internet. What it requires is less collection than validation. There are many more consumers, in principle ranging to cops on the beat. Given the dominance of the United States in conventional military power, virtually all the threats it faces – from states but especially from non-state groups like terrorists, will be asymmetric, the tactics of the weak. Thus, the feedback loop between what we do and how they respond will be tighter, a challenge for intelligence. One U.S. secretary of defense famously remarked about U.S. and Soviet nuclear programs: when we build, they build; when we stop, they build. Non-state adversaries cannot be assumed to be so predictable, or so entirely driven by their own internal imperatives.

States will remain the dominant actors in the international system, and will accordingly be major targets for intelligence. Some of those, like Iraq under Saddam or North Korea now, were and are hard and important targets even though they were weak or failed states. Others, like Iran, are more powerful and remain secretive. The most important state targets, like China and India, bode to be increasingly open. Yet, to the extent that states yield pride of place as intelligence targets to non-state groups, like terrorists, the challenge for intelligence is very different. Table 1 summarizes – and perhaps sharpens – those differences:

**Table 1**

**Traditional Targets Versus Transnational Ones**

| Traditional Targets | Transnational Targets |
|---|---|
| Focus: states, non-states secondary | Focus: non-states, states as facilitators, willingly or not |
| Nature of targets: hierarchical | Nature of targets: networked |
| Context: intelligence and policy share basic "story" about states | Context: much less shared story about non-states, less "bounded," more outcomes possible |
| Information: too little information, pride of place to secrets | Information: secrets matter, but torrents of information, fragmented |
| Reliability: secrets regarded as reliable | Reliability: information unreliable |
| Pace of events: primary target slow moving, discontinuities rare | Pace of events: targets may move quickly, discontinuities all too possible |
| Interaction effects: limited | Interaction effects: "your" actions and observations have more effect on target's behavior |
| Need for collaboration: limited, analysis in "stovepipes" | Need for collaboration: greater with both regional and functional intelligence specialists, plus different levels of government |
| Policy support: consumers mostly politico-military officials of federal government | Policy support: wider range of consumers, intelligence often linked to action on a continuing basis |

**From Drivers to Implications for Intelligence**

Against this backdrop, Figure 3 displays the logic of moving from drivers to their principal effects:

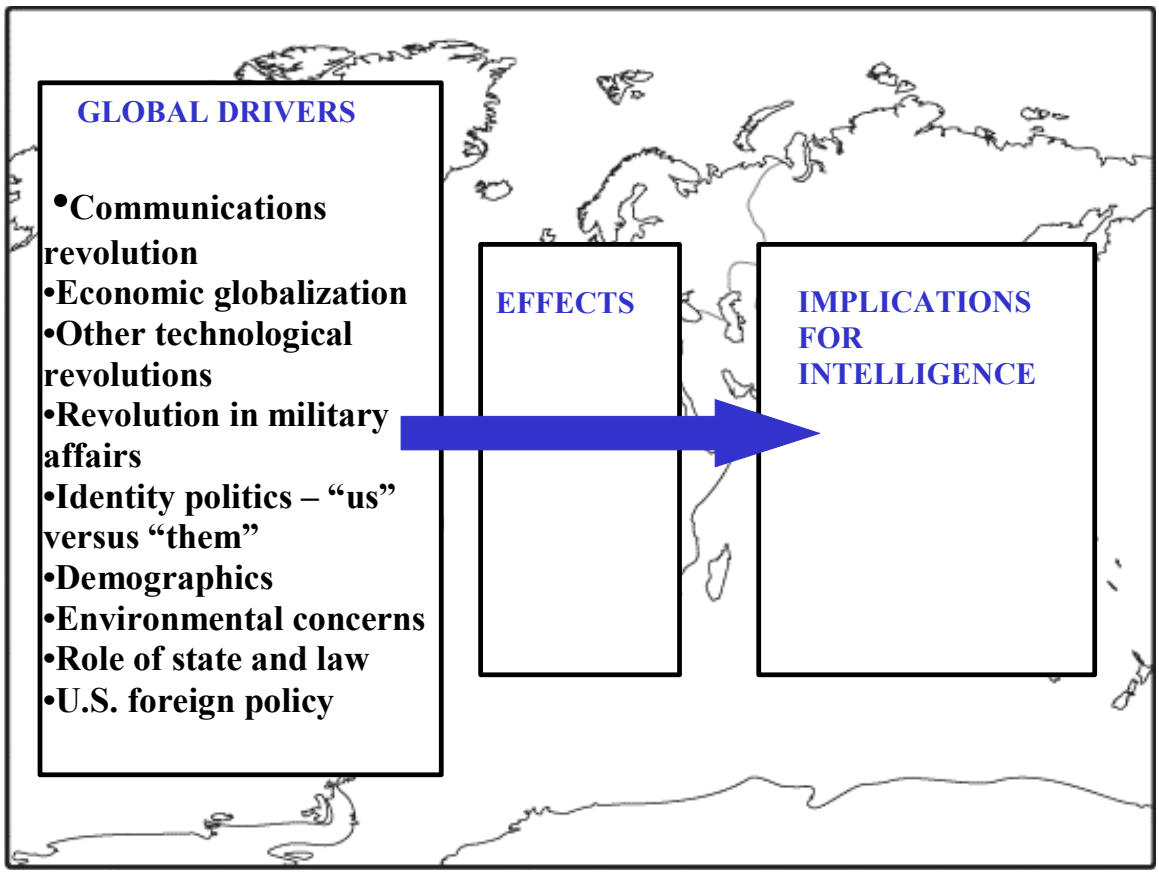



**Fig. 3—From Drivers to Implications for Intelligence**

Table 2 Summarizes The Effects and Implications, Driver by Driver:

**Table 2**

| Driver | Principal effects | Implications for intelligence |
|---|---|---|
| *Communications revolution* | Shifts comparative economic advantage<br>Enables civic action and terrorism communication<br>Segments populations<br>Increased vulnerability of U.S. as very dependent – very broad set of users | Harder targets – encryption, packet switching, volume<br>More targets = more opportunities<br>Need to get enter or get close to targets: DO in service of NSA<br>Dedicated warfighter systems, but sensors perhaps same<br>Feed-backs almost instantaneous |
| Economic globalization | Quality of people matter more; resources, distance much less<br>Gap between haves and have nots grows, at least in medium run<br>Makes United States the biggest target of grievance | "Bads" move as quickly around world as goods<br>Government policies constrained; but<br>Private actors – businesses and NGOs – more important<br>Asia biggest "winner," hence more important target<br>New rules – and perhaps new monitoring tasks – for international commerce |
| *Revolution in military affairs* | Network manages precision strikes from afar, linked to an array of sensors<br>Soldiers as sensors as much as shooters<br>U.S. in class by itself<br>Sensors and procedures for policing and contingency operations improve but more slowly | Need for warning against "leapfrogging" by potential adversaries, more in doctrine than technology<br>Rise in espionage against U.S. government and defense contractors<br>Much closer cooperation between intelligence and military in operations |

**Table 2 (Continued)**

| Driver | Principal effects | Implications for intelligence |
|---|---|---|
| *Identify politics – "us" versus "them"* | Divides "them" and "us" in new ways<br>Makes for less loyalty to state (or market)<br>Feeds new kinds of terrorism<br>Abets clash of civilizations | Need to monitor internal stability – requires language but more, deep cultural understanding<br>Changes are long cycle<br>Requires dealing with new kinds of threats – non-states driven by religion or other passions<br>Also produces more divided American society |
| *Other technological advances – biotech, nanotech and materials* | Genomic profiling, biomedical engineering, genetic modification – but also divides societies<br>"Smart," sensor-rich products<br>Nanotechnology changes the way things are designed and made<br>High-tech dominance of U.S. corporations but may wane | DNA, blood, genetic analysis advanced<br>New sensors aid tracking bad items and people, but deception also facilitated<br>"Tagging" property or items also permits targeting of agents<br>Increase in espionage and cyber crimes directed against U.S. corporations<br>Improved sensors and new testing raises civil liberties concerns |
| Global demographics | Global growth slows<br>Rich countries age, even shrink, some poor continue to grow<br>"Youth bulges" arise, especially among males, in some key countries | Labor shortages, including for military, arise in many countries, though not the United States<br>Youth bulges" threaten stability in key countries<br>But Asian countries face demographic "cliff"<br>Pressure to migrate increases<br>Imposes need to deal with failed or failing societies |

**Table 2 (Continued)**

| Driver | Principal effects | Implications for intelligence |
|---|---|---|
| Environmental concerns | Tipping points and catastrophes occur<br>Some crises will be global or regional, not national | Need to monitor trends, such as China's food (or energy) security<br>Rises or falls on government agenda, somewhat unpredictably |
| Changing role of state and law | Global economy, technology empower non-state actors, from terrorists, to corporations, to NGOs<br>Role of state, including U.S., becomes that of coalition-builder<br>International law continues to shift from states as subjects to people | Need to cooperate with a wide variety of states and non-states<br>Intelligence perhaps subject of special scrutiny, abroad and at home |
| U.S. foreign policy | Asymmetric foes will "morph" in response to U.S. actions<br>Broader actions will shape climate for cooperation with partners | Tighter coupling between "our" actions and threats we face – more need to know "blue team"<br>Agenda will change with U.S. policy |

Virtually all the drivers suggest that terrorism will not go away even as – perhaps in part because of – the continuing force of globalization. To be sure, states will remain the biggest actors in the international system, but the targets of intelligence will be more in number and more dispersed. Volumes of information will become more and more overwhelming, so the need for processing of all kinds – from what machines can do to analysts with deep understanding – will grow. The boundaries between the Intelligence Community and the rest of government and society will become lower, making for more competition but also new possibilities for partnerships in assembling information, even in gathering it. All the will take place as the drivers suggest the need, too, for more intelligence at home, even as those same drivers make for more international scrutiny of actions by states within their borders.