Science AND Technology TO Counter Terrorism

Science and Technology to Counter Terrorism

Proceedings of an Indo-U.S. Workshop

Roddam Narasimha and Arvind Kumar, *Editors*
Stephen P. Cohen and Rita Guenther, *Editors*

Committee on International Security and Arms Control

NATIONAL ACADEMY OF SCIENCES
THE NATIONAL ACADEMIES

In cooperation with
INTERNATIONAL STRATEGIC AND SECURITY STUDIES PROGRAMME
OF THE NATIONAL INSTITUTE OF ADVANCED STUDIES
Bangalore, India

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Council of the National Academy of Sciences. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This report was supported by Task Order No. N00014-05-G-0288, DO#9 between the National Academy of Sciences and the Office of Naval Research. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

Library of Congress Cataloging-in-Publication Data

International Standard Book Number (13): 978-0-309-10499-9
International Standard Book Number (10): 0-309-10499-8

A limited number of copies are available from the Committee on International Security and Arms Control, National Academies of Science, 500 Fifth Street, N.W., Washington, DC 20001; (202) 334-2811.

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu

Printed in the United States of America.

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph Cicerone and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

.

U.S. NATIONAL ACADEMY OF SCIENCES
COMMITTEE ON INTERNATIONAL SECURITY AND ARMS CONTROL

Raymond Jeanloz, University of California, Berkeley, *Chair*
John F. Ahearne, Sigma Xi
William F. Burns, U.S. Army War College
Ashton B. Carter, Harvard University
Christopher F. Chyba, Princeton University
Stephen P. Cohen, The Brookings Institution
David R. Franz, Midwest Research Institute
Richard L. Garwin, BM Thomas J. Watson Research Center
Rose Gottemoeller, Carnegie Endowment for International Peace
Margaret A. Hamburg, Nuclear Threat Initiative
Alastair Iain Johnston, Harvard University
Gerald F. Joyce, The Scripps Research Institute
Richard W. Mies, Hicks & Associates
M.T. Clegg, University of California, Irvine, *Ex Officio Member*

ORGANIZING COMMITTEE OF THE SCIENCE AND TECHNOLOGY TO COUNTER TERRORISM WORKSHOP

Kumar Patel, University of California, Los Angeles, *Chair*
Stephen P. Cohen, The Brookings Institution
Richard L. Garwin, IBM Thomas J. Watson Research Center
Rose Gottemoeller, Carnegie Endowment for International Peace
John P. Holdren, Harvard University
Jonathan D. Pollack, The RAND Corporation

Staff

Patricia Wrightson, Senior Program Officer, National Research Council
Rita S. Guenther, Senior Program Associate, National Research Council
Stacy Speer, Senior Program Assistant, National Research Council

INTERNATIONAL STRATEGIC AND SECURITY STUDIES PROGRAMME
NATIONAL INSTITUTE OF ADVANCED STUDIES
Bangalore, India

V. K. Aatre, Scientific Advisor to Raksha Mantri and Secretary to Department of Defense Research and Development, Ministry of Defense
N. Balakrishnan, Science and Engineering Research Council, Indian Institute of Science, Bangalore
Kalyan Banerjee, Former Defence Research Development Organisation Scientist
Vijay Chandru, Strand Genomics
S. Gopal, Associate, National Institute of Advanced Studies
Major General (Retd.) Afsir Karim, Security Analyst, New Delhi
Y.P. Kumar, Department of Science & Technology
Brig. A.S. Lamba, Deputy Director General of Perspective Planning
Rear Admiral (Retd.) Raja Menon, Security Analyst, New Delhi
Arrabida Mitra, Department of Science & Technology, New Delhi
T.G.K. Murthy, Department of Space
Roddam Narasimha, Director, National Institute of Advanced Studies
M.K. Narayanan, Center for Security Analysis, Chennai
P.C. Pandey, Director, National Center for Antarctic and Ocean Research, Goa
M. K. Paul, Controller, National Institute of Advanced Studies
P. Rama Rao, International Advanced Research Centre for Powder Metallurgy and New Materials, Hyderabad
S. Rajagopal, Homi Bhabha Visiting Professor, National Institute of Advanced Studies
V.S. Ramamurthy, Secretary, Department of Science & Technology
B. Raman, Institute of Topical Studies, Chennai
M.K. Rasgotra, Former Foreign Secretary, Government of India
Julio Ribeiro, Former Police Commissioner, Punjab
Gen. S. Rodrigues, Former Chief of Army Staff
K. Santhanam, Director, Institute for Defence Studies and Analyses
V. Siddhartha, Defence Research Development Organisation, Headquarters
G.R. Srinivasan, Former Atomic Energy Regulatory Board Scientist
R. Varadarajan, Head, Administration, Department of Science and Technology
Zingde, Director, National Institute of Oceanography

National Institute of Advanced Studies Staff

Maj. Gen. M.K. Paul (Retd.), Controller, National Institute of Advanced Studies
Arvind Kumar, Research Faculty, International Strategic & Security Studies

Preface

These proceedings present the papers and summarize the discussions of a workshop held in Goa, India, in January 2004, organized under the aegis of the Indian National Institute of Advanced Science (NIAS) and the U.S. Committee on International Security and Arms Control (CISAC). NIAS is an independent research institute located on the campus of the Indian Institute of Science in Bangalore, and CISAC is a standing committee of the U.S. National Academy of Sciences (NAS). The two groups have had an ongoing bilateral dialogue since 1999.

In four meetings held before the workshop, NIAS and CISAC addressed such subjects as the future of nuclear arms control, nuclear doctrine and operational practices for nuclear weapons, protection and accounting of nuclear explosive materials, Indian-U.S. cooperation in science and technology, and security developments in South Asia and other regions.

From the early planning stages of this project, CISAC and NIAS searched for a workshop topic that could be explored in greater depth, a topic of relevance to scientists, experts, and the broader policy communities in India and the United States. In 2001 it was agreed that the topic of this workshop, how science and technology can be used to counter terrorism, was of great importance and great timeliness. By the 2003 planning meeting in Bangalore, terrorism had become an issue of central concern for the United States, as it had been in India for some time. Terrorism was an issue that deeply concerned both countries. Workshop organizers therefore decided to attempt something tangible as a next step in the NIAS-CISAC dialogue by seeking to meet three objectives during the joint event.

First, we wanted to better understand the nature of the terrorist threat that we faced in both countries and elsewhere in the world, and how it became a global phenomenon. Our hope was that this workshop might better prepare Indian and U.S. specialists to work together to counter the networks now responsible for a variety of terrorist attacks across the globe.

Second, we specifically wanted to see how science and technology could help in the fight against terrorism, and therefore this question became the framework for the workshop. We were conscious of the fact that science and technology alone will not solve the problem. For this reason, the workshop included those who had dealt with the realities of terrorism from perspectives beyond those of the more traditional science and technology communities. Nevertheless, science and technology can be of great

assistance if properly employed, and we wanted to jointly explore the best ways to identify the areas where it can be most effective.

Third, NIAS and CISAC wanted to explore opportunities for the United States and India to work together. We recognized that terrorism is a common problem, although it may manifest itself in different ways in the U.S. and Indian contexts. Even allowing for differences between our countries, what are the opportunities for specific cooperation? We wanted to use this meeting as a catalyst for people—scientists as well as other experts—from the two countries to come together and identify areas for joint research and, potentially, for joint action. Following the terrorist attacks of September 11, 2001, U.S. officials publicly invited ideas and proposals from across the world. We hope that the proposals and ideas discussed at the workshop, and presented below, might contribute to ways in which both countries can better tackle the problems created by terrorism.

Terrorism is not a new problem. However, terrorists now employ science and technology to conduct terrorist attacks across national boundaries. Despite its international reach, the manifestations of terror differ from location to location. It was this contrast of the similarities yet differences that made this particular workshop so beneficial. Bringing together scientists and experts with common scientific and technical backgrounds from different cultures provided a unique opportunity to explore possible means of preventing or mitigating future terrorist attacks. Although there is great hope that the judicious deployment of science and technology will make it difficult for terrorists to conduct further acts of violence, as scientists we recognize that 100 percent protection is not possible.

The agenda of the workshop was driven by the desire to maximize the experience and expertise of the Indian and American participants, and to lay the groundwork for long-term collaboration. All of the sessions and their accompanying discussions, and particularly the last session, explored areas for the United States and India to collaborate in the future.

The workshop was organized into five sessions. Session I surveyed the terrorist threats in the United States and in India and relevant science and technology tools available in each country. Sessions II-IV covered the following specific themes: threats to information technology and communications, vulnerabilities of urban and infrastructure targets, vulnerability of nuclear power facilities, and risks to human and animal health from bioterrorism. The final session gave us an opportunity to explore the question, "Where do we go from here?"

Our expectations were that the workshop would yield a deeper understanding of terrorist threats to our respective countries, and identify steps by which science and technology can deter, prevent, monitor, mitigate, respond to, and recover from potential terrorist acts. Many valuable insights on countering terrorism were gained through the joint workshop and remain valid and relevant even some time after they were originally discussed. These insights have been captured in the papers presented throughout these proceedings.

We also wanted to identify future joint activities. These need not be carried out under the auspices of NIAS or CISAC, and our goal was to suggest two or three such activities to be pursued by the broader Indian and U.S. science and technology communities. Our belief is that the proceedings of this workshop demonstrate the great value in both clarifying the nature of the threat and developing ideas for future

cooperation to address that threat. The underlying premise of this entire project is that terrorism can be addressed more effectively if there are cooperative and multilateral efforts by affected states, rather than a series of uncoordinated activities by individual states.

The statements made and views expressed are solely the responsibility of the authors and do not represent the positions of the Office of Naval Research, the National Academy of Sciences (NAS), NIAS, or other organizations where the authors are employed.

Acknowledgments

This publication was made possible by a grant from the Indo-U.S. Science and Technology Forum and by the Office of Naval Research, and in India by the National Institute of Advanced Studies, Bangalore.

This volume has been reviewed in draft form by several individuals chosen for their technical expertise, in accordance with procedures approved by the NRC's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in ensuring that the report is as sound as possible and meets institutional standards for quality. The review comments and original draft manuscript remain confidential to protect the integrity of the process.

We wish to thank the following individuals for their review of selected papers: Edward Badolato, Integrated Infrastructure Analytics, Inc.; Carol Blair, Colorado State University; David Borth, Motorola Inc.; Siegfried Hecker, Stanford University; Raphael Perl, Congressional Research Service; S. Rajagopal, National Institute of Advanced Studies, India; R. Rajaraman, Jawaharlal Nehru University; and Basheerhamad Shadrach, International Development Research Centre.

Although these reviewers have provided constructive comments and suggestions, they were not asked to endorse the content of the individual papers. Responsibility for the final content of the papers rests with the individual authors.

We wish to thank the following individuals for their cooperation and support, and for their assistance in making the workshop possible and subsequently in producing these proceedings. Dr. Roddam Narasimha and Dr. Kumar Patel served as co-chairmen of the workshop, ensuring the success of the joint NIAS-CISAC event that led to this rich volume and opened the path for further cooperation between scientists from India and the United States. Dr. Stephen P. Cohen served as a skilled editor of the early drafts of the manuscript, crafting passages as deftly as a diplomat and as carefully as the dedicated scholar that he is. Arvind Kumar, a Research Faculty Member at NIAS, was instrumental in completing these proceedings. Without his tireless dedication, diligence, and cooperation with NAS staff, the final publication of these proceedings would not have been possible. The hard work and systematic approach of Ms. Rita Guenther of CISAC, NAS, helped in bringing about this publication. She worked around the clock on this publication since July 2006. It would not have seen the light of the day without her persistence, experience, and understanding.

Contents

1

Science, Technology, and Countering Terrorism: The Search for a Sustainable Strategy

Lewis M. Branscomb

The scientific and research policies of the U.S. government were profoundly transformed by the cold war in response to a military strategy of technological superiority.[1] Only the shock of the September 11, 2001, attack on the World Trade Center, the Pentagon, and one other unknown target forced a restructuring to meet the threat of catastrophic terrorism.[2] This paper addresses the nature of that threat and the role that science and technology can play in mitigating the risk and the consequences of such attacks. The conclusion summarizes the impact on science and technology policy that may result. A serious constraint on that policy is the need for a sustainable and affordable strategy, which the private sector as well as government will adopt and which the public will support for many years into the future.

This presentation addresses four questions:

1. How different is the current threat from that for which the institutions of government are primarily structured?

[1] This paper is drawn heavily from National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, D.C. The report is available in PDF format at *http://books.nap.edu/hml/stct/index.html*. This paper offers the author's own views, for which the National Research Council is not responsible.

[2] "Catastrophic terrorism" is distinguished from destructive acts of lesser consequence by the nature of the societal response appropriate to the threat. It is assumed that the criminal justice system is adequate to deal with most lesser threats, even those that cause a great deal of public concern, such as the sniper attacks in suburban Maryland and Virginia in October 2002. The September 11, 2001, attack sets a new standard for severity of consequence, in both human life and economic damage. We can also imagine terror attacks such as the detonation of a radiological contamination weapon causing levels of panic and loss of confidence in the government's protection of its citizens thereby constituting a catastrophe. Also repetition of smaller but deadly attacks, such as suicide bombings in Israel, can accumulate to create a sense of extreme anxiety in the population.

2. How can science and engineering contribute to making the nation safer against the threat of catastrophic terrorism?
3. Where will the responsibility lie for defining those responses, investing the needed resources, and implementing the strategies?
4. How can a strategy for mitigating the threat of catastrophic terrorism be sustainable in a democratic society whose political system is known for its short attention span?
5. Given the reality that most of the targets of terrorism are privately owned, and many of the vulnerabilities are the result of firms maximizing efficiency at the expense of security externalities, how can a public-private balance between private efficiency and public vulnerability be found?

THE TERRORIST THREAT TODAY

To understand how science and technology might contribute to countering terrorism, we must evaluate the nature of the threat, the vulnerabilities of targets in civil society, and the availability of technical solutions to address the vulnerabilities that are most likely to be exploited by terrorists.

India and the United States, the world's two largest democracies, are both vulnerable to terrorist attacks. As an Indian participant in the workshop said, "The most vulnerable states are those with open societies that tolerate dissent." So far, India and the United States have faced rather different forms of terror attacks.

Let me distinguish two forms of terrorism, which I shall categorize as tactical and strategic. Tactical terrorism is characterized by the use of conventional small arms weapons plus explosives (often in the form of car or truck bombs) against individuals in an attempt to put political pressure on a government that has proved intransigent regarding the political objectives of the terrorists. India has experienced a great deal of this kind of terrorism, as has Israel, and the United Kingdom (from the military wing of the Irish Republican Army). Strategic or catastrophic terrorism, on the other hand, seeks to inflict maximum damage against targets that are ideologically despised by the terrorists. In this case the terrorists wish to draw attention to their cause, to inflict maximum damage on the legitimacy of a government, and to inflict major economic penalties on the nation or nations in question. The attack on the World Trade Center by al Qaeda fit this pattern, as did the attack in the Tokyo subway by the Aum Shinrikyo. Such terrorists do not seek to shock a government into making concessions through negotiation.[3] Thus the U.S. concern for catastrophic or strategic terrorism is different—and presents a broader spectrum of opportunities for science and technology to reduce the nation's vulnerability—than is the case today in India. However, given the demonstration of catastrophic destruction in the September 11, 2001, attack in New York City, India, like the United States, a nation that plays an important role in the world, must assume that the day will come when such attacks might be inflicted upon her. The

[3] There is, of course, no clear line between these two types. Guy Fawkes's attempt to blow up the Houses of Parliament in London in 1605, the destruction of the Reichstag, attributed to Hitler's brown shirts, and the Chechen attack on the "Palace of Culture" in Moscow in October 2002, lie somewhere in between these two types.

United States may also find itself the victim of suicide bombers and truck bombs (as indeed it was in the attack on the Alfred P. Murrah building in Oklahoma City in April 1995).

Terrorists possess some advantages, despite their small numbers. First, their actions are largely unpredictable, since their objectives, at least those of ideological terrorists such as al Qaeda and Aum Shinrikyo, are largely idiosyncratic and obscure.[4] Second, the terrorists must be assumed to have some part of their number in covert residence within the societies they plan to attack. Third, terrorists appear to be very patient. They decide when they will strike. As a result, those defending against terrorism must be alert at all times, despite the apparent absence of visible terrorist activity. Finally, terrorists may have international bases of operations, and quite possibly enjoy the sponsorship and assistance of a rogue state. This combination of stateless terrorists who infiltrate target societies, supported by the resources of an irresponsible but technically competent foreign government, is a particularly dangerous combination. The U.S. government identified the Taliban government of Afghanistan as such a state. The U.S. administration was obviously concerned that the Baathist government of Iraq might also represent such a state, although there is no credible evidence that Saddam Hussein had anything to do with the September 11, 2001 attack.[5]

Notwithstanding the terrorist threat, modern industrial societies have some offsetting advantages. Their global intelligence services and military presence, especially when they cooperate with one another, may keep the terror networks off balance, and may be able to damage some of them and interfere with their communications and money flows. Military action, or the threat of it, may discourage rogue states from supporting the terrorists. Nevertheless, highly efficient economies also acquire vulnerabilities and reduced resilience from the private sector's reluctance to sacrifice efficiency to reduce catastrophic risks whose likelihood is difficult to estimate.[6]

One area in which both India and the United States enjoy impressive capability is research and innovation. Through the application of available or new technologies, states can make targets less vulnerable, thus less attractive. They can limit the damage that may result from an attack, increase the speed of recovery, and provide forensic tools to identify the perpetrators. However, terrorist networks such as al Qaeda are led by well-educated and well-financed people who may also enjoy advanced technical skills. If supported by a government whose military establishment has developed weapons of mass destruction, these skills may be greatly amplified. Any technical strategy for responding to the threat of catastrophic terrorism must address this fact.

---

[4] Politically motivated terrorists, such as the Irish Republican Army, may have a specific goal, which, if achieved, might bring an end to their attacks. We can imagine an attempt to negotiate an end to their terrorism. This is not the case for the al Qaeda terrorists who carried out the September 11, 2001 attack on New York City and Washington, D.C.

[5] Gerald Holton anticipates just such a combination of individual terrorists supported by a rogue government in a paper presented at a terrorism conference at the Hoover Institution in 1976 and published at that time in *Terrorism*, an international journal. He called this threat Type III Terrorism. See, Holton, Gerald. 2002. "Reflections on Modern Terrorism," *Edge.* Available online at *http://www.edge.org/3rs_culture/holton/holton_print.html.*

[6] Auerswald, Philip, Lewis M. Branscomb, Todd LaPorte and Erwann Michel-Kerjan. 2006. *Seeds of Disaster, Roots of Response: How Private Actions can Reduce Public Vulnerability,* Cambridge University Press, New York.

THE THREAT OF CATASTROPHIC TERRORISM

Any strategy for employing technical knowledge and systems to reduce the likelihood or consequence of catastrophic terrorism must be able to estimate

- the terrorists' goals and priorities
- the most vulnerable targets among those priorities
- the weapons most desired by and available to the terrorists and the consequences of their use
- the effectiveness of available means to either deter an attack or reduce its consequences

Terrorists' Goals and Priorities

The targets selected by terrorists will depend on their goals and opportunities. Terrorists may be expected to choose among six objectives:

1. inflict extensive loss of human life
2. destroy important, difficult-to-replace physical facilities
3. exact severe economic damage for a persistent time
4. disrupt the institutions of government
5. attack the symbols of civil culture most detested by the terrorists
6. boost the morale and enhance recruiting of terrorist groups

The September 11, 2001 attack by al Qaeda was designed to create significant damage in all six areas and succeeded in doing so. However, their primary goal seemed to be a combination of the first and fifth objectives. Their success in wreaking economic havoc in the U.S. airline industry and in the economy as a whole appears to have been an unanticipated bonus.

The Targets

The physical facilities in which large numbers of people are concentrated are primarily in big cities. So too are many of the industrial facilities whose destruction might inflict both economic damage and human injury if toxic substances are released. These buildings and factories are largely owned by private businesses, especially in the United States. Transportation facilities—airports, bridges, dams, tunnels, and so forth——are typically owned by municipal, state, or national authorities. Thus, the responsibility for protecting the primary targets is shared among private and government owners, and on the government side, among national, state, county, and municipal authorities.

The targets of catastrophic terrorist attacks may be organized into these seven categories:

1. people who are vulnerable to infectious disease, toxic chemicals, or radiation delivered either directly or through contamination through food, currency, postage stamps, or other means of distribution to individuals
2. communications and information services, especially those services essential to command and control centers, and to protection and recovery of complex industrial systems
3. energy systems (power plants, refineries, and both fuel and energy distribution systems)
4. transportation systems (air, sea, and land, both mobile and fixed infrastructure for transportation—tunnels, bridges, harbors)
5. cities and fixed infrastructure and the people who inhabit them (office buildings, water supplies, dikes)
6. facilities where many people may be congregated at high density (as in athletic venues and theaters)
7. indirect impact on economies through disruption of critical infrastructure services

In a modern industrial society, how vulnerable are these targets?[7] Both "critical infrastructure" service industries and structures housing large numbers of people are vulnerable. These are not created by the terrorists, but may be exploited by them. They are, instead, created by the quest for increased efficiency in a competitive, market economy. The competitive drive for commercial efficiency not only creates vulnerabilities in each critical service industry but also creates linkages among these critical infrastructure industries—energy, transportation, communications, food production and distribution, public health, and financial transactions are all interdependent.

The mechanisms through which the quest for industrial efficiency may threaten industry's resilience to catastrophic terrorism include

- single-point failures, where costs of adding redundant elements are high and risks from small perturbations are low, such as ultra-high-voltage transformers in electric power distribution
- excessive concentration in the quest for scale economies (concentration of chicken meat processing and distribution in a handful of large firms; aggregation of fuel and passengers in ever larger commercial air transports such as the Airbus 380 with up to 850 passengers, and ever larger ocean liners such as the new cruise ship under construction for Royal Caribbean Cruise Lines, designed for 6,400 passengers)
- coupling of critical infrastructure systems to leverage their scale economies (dependence of transportation safety on availability of electric power and secure computer networks; the dependence of the electric power system on the integrity and security of computer networks)

The single-point failures of some critical industrial infrastructures are vulnerable

[7] The issue of reducing the vulnerability of critical infrastructure has been extensively studied in a new book, *Seeds of Disaster, Roots of Response,* cited above.

to widely available, conventional weapons, such as explosives, assault rifles, and rocket-propelled grenades. Others may be attacked with more potent weapons made from the very products, materials, and systems of a modern industrial economy.

Terrorists' Weapons

The weapons terrorists might use are divided into two classes: weapons of mass destruction (WMD) and weapons derived from the very economy under attack. WMD can, in principle, be fabricated by technically skilled terrorists, but more probably will originate in rogue states covertly supporting the terrorists or perhaps are stolen from military supplies of more advanced nations.[8] These WMD are nuclear, biological, and chemical weapons[9] designed initially for military use, and restricted (but not eliminated) by a series of treaties among many but not all nations. There are no more urgent issues for the future of civilization than the effective means for reducing the number and proliferation of WMD, the sequestering of those that remain, and the control of the materials from which they can be easily fabricated.

However, we must bear in mind that while weapons of mass destruction are generally the most lethal, they also tend to be the most inaccessible to terror organizations that are not assisted by a technically competent but irresponsible government. The terrorists who attacked the World Trade Center in September 2001 certainly created mass destruction, but the weapons used (fully fuelled airliners used as cruise missiles) were technically, at least under U.S. law, not WMDs.

The other class of weapons, those derived from the civil economy of the nation under attack, are more diverse, more numerous, and more accessible to terrorists. Examples include the nitrogen fertilizer (ammonium nitrate) and fuel oil such as that used in the April 1995 attack on the Alfred J. Murrah building in Oklahoma City, tank cars of chlorine being shipped to water supply utilities and other chemical plants, crop dusters that might be used to disperse chemical agents, and fully fuelled aircraft such as used in the September 11, 2001 attack. A more complete list of terrorists' weapons includes

- fissile nuclear materials, tactical nuclear weapons, and radiological materials
- pathological organisms (human, plant, and animal)
- military-type toxic chemical weapons
- inflammable, toxic, and explosive chemicals and materials in industrial use
- cyberattacks and electromagnetic pulse (EMP) attacks on electronic targets (telecoms, data, or command and control centers)
- transportation systems used as delivery systems for weapons
- explosives, either conventional or derived from fuel oil and nitrogen fertilizer (ammonium nitrate), for example

[8] "Rogue" is used loosely here to refer to states that make WMD available to terrorists, either through deliberate policy or through failure to protect their stocks of weapons (and the talent for making them) from losses through theft and corruption.

[9] In the United States the legal definition of weapons of mass destruction includes not only fissile materials and nuclear explosives but also radiological weapons. However, radiological weapons (so-called dirty bombs) are weapons of mass terror, as the destruction caused by a detonation would be largely confined to the explosives used to disperse the radioactive material.

Protecting Nongovernmental Infrastructure

Who will pay to harden nongovernment-owned critical infrastructure and the critical services it supports? There are a variety of possible policies to motivate private investments in hardening of critical infrastructure. Some of them are

- compulsion through regulation (which may require congressional legislation)
- subsidies of the research and development to design the hardening strategies through public-private research and development partnerships (but this still leaves industry with the capital expense for implementing the strategy)
- voluntary commitments with antitrust exemption (the chemical industry in the United States has an excellent record of voluntary standards for plant safety, which might become a model for protection from terrorism, although the industry has lobbied hard, and effectively, against mandatory regulation for security)
- inducing the insurance industry to set a sliding scale of rates for terrorism loss insurance, reflecting the extent to which client firms have adopted hardening measures

Unfortunately, little progress has been made by the U.S. federal government toward defining the tools to be used in each of the areas of critical industry. The U.S. government is now proceeding on a case-by-case basis, focusing primarily on how to motivate the large pharmaceutical companies to manufacture vaccines for which there is no "peacetime" market. But no general strategy for the permanent hardening of the U.S. economy has been adopted.[10]

In a limited number of cases, firms may be able to devise hardening strategies that also reduce costs or improve product or service value so that the total costs are minimized or are even negative. The manner by which many firms responded to the Y2K threat offers some encouragement for this notion. Such a dual-use[11] strategy is needed to increase the likelihood that industry will invest in hardening critical infrastructure, to create a more sustainable public commitment to the costs and inconveniences of national efforts against terrorist threats, and to integrate homeland security research and development with the rest of the societal research and engineering base to ensure a fully national effort of high-quality results.

Because most of the targets and many of the weapons are imbedded in the civilian economy, security issues cannot be neatly separated from the daily life of the civilian population. The strategy for gradually restructuring many of our physical facilities, production processes, means of providing food distribution, and the like, will have to reflect a complex balance of public-good investments (for which government will have to take the initiative), and commercial investments aimed at competitive success. The political economy of the United States is not designed to make this marriage of

[10] The National Infrastructure Protection Plan (NIPP) has been issued by the Department of Homeland Security and many other government departments, but it does not effectively solve the problem of motivating the private sector to invest in vulnerability reduction. See *www.dhs.gov/NIPP*.

[11] Ruth A. David, CEO of ANSER Corporation, correctly suggests that "dual benefit" would be a more appropriate phrase in this context.

conflicting interests and responsibilities easy; India, European nations, and some Asian economies are more accustomed to this balance in their economies. However distasteful the phrase ideologically, the U.S. government needs a counterterrorism industrial policy.

Examples of civilian benefits that might result from such a strategy are

- revitalization of the public health service for serving the normal health needs of communities
- technical capability to respond even faster and more effectively to natural biological threats such as Severe Acute Respiratory Syndrome (SARS), West Nile virus, and monkey pox virus
- reduction in the number of illnesses caused by infection or poisoning of the food supply
- more reliable electric power and other services, especially in the face of hurricanes, floods, and earthquakes
- further improvements in the safety standards of the chemical industry
- reduced incidence of cyberattacks by hackers and financial systems made more secure against theft and malicious damage
- more efficient and timely tracking of goods in transit and billing for their content
- reduced risk to fire, police, and emergency health professionals

MITIGATION: THE ROLE OF SCIENCE AND TECHNOLOGY

The U.S. National Academies report *Making the Nation Safer* made more than 130 recommendations for ways to prevent and respond to terrorist attacks. Listed here are a few examples of specific threats and the corresponding recommendations for the use of science and technology to address those threats.

Nuclear and Radiological Threats

If terrorists with a minimal level of scientific knowledge can acquire enough highly enriched uranium (HEU), they may be able to assemble an inefficient but effective nuclear weapon for detonation in a major city. The United States and Russia are now cooperating in safeguarding fissile material and blending down stocks of HEU, but progress is far too slow. Even more dangerous is the possible availability to terrorists of finished nuclear weapons either stolen and sold from nuclear states or provided by rogue states capable of making them.[12]

The U.S. public must be educated on the nature of radiological threats, both from Radiation Dispersal Devices (dirty bombs) and from damaged nuclear electric power plants and radioactive waste storage. Public ignorance about radiation hazards may

[12] Americans are perhaps more nervous than their friends in India about the political instability of the Pakistani government and the possible consequences should Pakistani nuclear weapons or weapons materials find their way into the hands of terrorists hostile to the United States. Today, attention is shifting to North Korea and Iran as potential sources of weapons or materials, both of which apparently obtained technology from Pakistan.

induce a level of panic much more destructive than the radiation from which people may be fleeing.

The technical task of detecting fissile materials being covertly shipped into a target state is a daunting task, and is receiving a high level of research attention in the United States, but can never be depended upon to stop the import of material for a single weapon. Only control at the source will suffice.

Biological Threats to People and Their Food Supply

Research on pathogenesis of infectious agents, and particularly on means for early detection of the presence of such pathogens before their symptomatic appearance, is important. Nations will stockpile vaccines against known diseases, but the threat of genetic modification—while perhaps beyond the capability of most terrorists but not of rogue states—requires a vigorous research effort to find solutions for detection, evaluation, and response.

In the United States the Center for Disease Control and Prevention (CDC) provides a robust capability in epidemiology, but there is no equivalent epidemiological response capability for possible biological attacks on agriculture and farm animals. Thus, measures to protect the food supply, and to provide decontamination after an attack, must have high priority.

Toxic Chemicals, Explosives, and Flammable Materials

Some highly lethal chemicals, such as those made for military applications, are relatively easily made from widely available materials. There is even greater risk from industrial chemicals, which are widely accessible as they move in commerce. Dangerous chemicals in transit should be tracked and identified electronically. To ensure that only first responders, and not terrorists, know what the tank cars contain, the rail cars should be equipped with encrypted electronic identification.

Sensor networks are required to detect and characterize dangerous materials, particularly when they are airborne. Self-analyzing filter systems for modern office buildings whose windows cannot be opened can not only protect the inhabitants but also detect and report the first presence of materials (such as aerosols) that may be trapped in improved filters. An example of long-range, basic research that could be highly beneficial would be the discovery of olfactory biosensors than can reach dog levels of sensitivity, some 10,000 times that of humans.

Energy Systems

The hazards associated with fossil fuel storage, shipment, and use are well known. Perhaps less apparent are the vulnerabilities of a modern electric power grid. Many of these systems have vulnerable, unique extra-high-voltage transformers for which there are no spares and thus represent a single-point failure. A solution recommended in *Making the Nation Safer* is the production of more portable and safely stored midsized transformers specifically designed to be reconfigurable in combination to replace a failed high-voltage transformer.

Another vulnerability results from the replacement of operating engineers in power distribution control rooms with computer systems running Supervisory Control and Data Acquisition (SCADA) systems. These computer-based software systems are generally produced abroad; it is difficult to guarantee their integrity. In addition, while some electric utilities use encrypted traffic on fiber optics to communicate among the SCADA computers, others use clear traffic on the Internet, vulnerable to a cyberattack. An experienced hacker might gain control of the SCADA system and use it to damage the power distribution system. From a longer time frame perspective, adaptive power grids should be developed to make them both harder to attack and make recovery after attack much easier and quicker.

Communications and Information Systems

In the United States the most urgent issue is to reconfigure first responder communications so that police, fire, and medical personnel can communicate with one another and with the emergency operations centers. Inability to do so greatly aggravated loss of life, especially among firefighters, in the World Trade Center attacks. The main worry about cyberattacks is the possibility of their use, perhaps with electromagnetic pulse devices as well, to amplify the destructive effect of a conventional physical or biological attack.[13] Cybersecurity is one of the top priority areas for research investment because private industry was, before September 11, 2001, largely content with the level of computer and network security available to it. A quite inadequate level of sophisticated talent is devoted to the goal of fully secure operating systems and networks.

Transportation and Borders

Sensor networks for inspection of goods and passengers crossing the nation's borders will be a research priority. The primary technical challenge will not be the design of sensors themselves, although much progress is needed in this area, but in the systems engineering of the networks of sensors together with data fusion and decision support software.

Biometrics for more secure identification of individuals shows promise, and systems superior to the driver's licenses and passports used by most travelers are promising.

The range of threats to the transportation networks of a modern state is very great, and careful systems analysis is essential to identifying the weak points and finding the most effective and economical means of protecting them.

Cities and Fixed Infrastructure

The Emergency Operations Centers (EOC) in many large U.S. cities are quite vulnerable, not only to a destructive physical attack but to more indirect attacks on their ability to access data and to communicate through a cyberattack or electromagnetic pulse attack. Remedying these vulnerabilities must have high urgency; in many cases the centers will have to be relocated. Tragically, the EOC in New York City was located in a

[13] *Making the Nation Safer*, p. 136-137.

known target, the World Trade Center.

Much research is already under way to analyze the structural characteristics of high-rise buildings that may make them much more vulnerable than necessary. Without waiting for this research to result in revised building codes, the expert panel recommended immediate adoption and extension, where appropriate, of European standards for fire and blast, which were much improved following World War II.[14]

As already noted, air intakes for large buildings need to be less accessible and equipped with better air filters, perhaps with chemical analysis sufficient to determine if a toxic material is present.

Instrumentation to allow first responders to detect toxic and hazardous materials; special provisions for protecting harbors, bridges, dams, tunnels, and dikes; and protection against attacks on urban water supplies downstream from the treatment plant are all discussed in *Making the Nation Safer*.

How much of the long term, imaginative research and development envisioned in *Making the Nation Safer* has been undertaken by the Department of Homeland Security (DHS)? Not enough. The Science and Technology Directorate of DHS does not have the scope of authority, nor the length of vision that the Academies' study urged on Congress. Critics say that it has been difficult for DHS to sustain an expert staff with low enough turn over to build and execute the needed technical strategies. Nor has the Homeland Security Institute been given the necessary scope of independent system-level review of the DHS technical priorities.

SOCIETAL RESPONSES TO TERRORIST THREATS

Making the Nation Safer concludes that public fear and confusion are more likely responses to most terrorist attacks than is terror, that is, a level of fear so intense that individuals are rendered incapable of acting rationally. The main dangers are panic and destructive behavior as a result of the lack of credible and timely public information. Thus, a loss of public confidence in those responsible for protecting the public can also be an attack amplifier. The government faces a number of dilemmas, such as using a color-coded warning system to alert the public to the perceived likelihood of additional terrorist attacks. Some citizens feel that this system itself may needlessly amplify the threat, thus doing terrorists' psychological job for them.

An urgent issue to be addressed is for government to train and introduce to the public, well in advance of any attack, a number of trusted and knowledgeable people who are prepared to provide accurate and trustworthy information quickly and authoritatively.

TECHNICAL STRATEGIES

From the great variety of threats studied by the National Academies' experts, several commonsense conclusions about technical strategy can be extracted:

[14] Ibid, p. 256.

- repair the weakest links (single-point failures) in vulnerable systems and infrastructures
- use defenses-in-depth (do not rely only on perimeter defenses or firewalls)
- use "circuit breakers" to isolate and stabilize failing system elements
- build security and flexibility into basic system designs where possible
- design systems for use by typical first responders
- focus priority attention on the "system of systems" technical challenge to understand and remedy the inherent weaknesses in critical infrastructure that are inherent in their architecture[15]
- ensure that first responders, including technical teams from critical infrastructure service industries, are properly trained and equipped, and the targets themselves are designed to be more resilient in the face of disaster
- emphasize the importance of flexibility and agility in responding to disasters that were not anticipated in the system design and personnel training

The last point is particularly important. Future attacks are likely to involve multiple complex systems. There are a number of dimensions to the systems engineering challenge of homeland security. The multiple critical industrial infrastructures are closely coupled. Almost all of the responses to terrorist threats require the concerned action of national agencies, state and local authorities, private companies, and in many cases, friendly nations. The technologies used in counterterrorism will themselves be coupled, complex systems. An evident example is the notion of complex networks of sensors that are coupled to databases, within which the network output is fused with other information, and from which sensible and useable information for local officials in Emergency Operations Centers must be provided. Thus, setting priorities requires modeling and simulating attack and response, and "red teaming" to test the effectiveness of proposed solutions.

Finally, there is a need to build up investments in the social sciences, which will be especially important in devising strategies for countering terrorism. Both the roots of terrorism and its consequences need to be better understood. Social science can also contribute to a sustainable effort, involving multiple levels of government, with minimal economic cost, and where the perceived conflict between security activities and protection of individual freedom can best be informed and adjudicated.

A SUSTAINABLE STRATEGY FOR HOMELAND SECURITY

Because major terrorist attacks against civil populations may be separated by considerable intervals of time, there is reason to be concerned that the public will lose interest in the threat, and that none of the organizational or investment needs will be satisfactorily met. For these reasons, the strategy for maximizing civil benefits deserves high-priority attention. There are many obvious examples of how counter terror research

[15] Note that the United States will find restructuring complex infrastructures to be very difficult and expensive, since these systems are not designed to permit easy restructuring. India has a window of opportunity in that much of its infrastructure is still relatively simple, but it is growing in size and complexity very quickly.

and development can create values appreciated by the public and of economic value to firms, such as creation of a more agile vaccine development and production capability, information and communications networks that are more resistant to cyber attack, energy systems more robust in the face of natural disasters and human error, security technologies that are more effective yet more unobtrusive and convenient for the public.

Sustainability will be a challenge for those in political power in the United States, for they find themselves compelled to emphasize the public's vulnerability (for example, with the color-coded alert system, which is largely successful in making the public nervous) and at the same time to emphasize that the government's efforts "have the terrorists on the run." Indeed, we can easily imagine that terrorist organizations such as al Qaeda may deliberately wait long intervals between attacks to decrease the alertness of the target's defenses.

Sustainability requires one additional strategic element that is of the highest importance. The compromises to civil liberties that the public will readily accept during a traditional war, which is expected to be of short duration, will not be acceptable in the context of a terrorism threat that knows no end, that offers no victory. Thus, the public must be very alert to the kinds of emergency legislation and exercises of executive authority that may be helpful in the short term, but carry the danger of concentrating too much political power in the incumbent government over an indefinite length of time.

There are two kinds of expressions of government authority that must be carefully constrained. One is specific legislation that may deprive individuals of constitutional rights, including rights that are found in the Supreme Court interpretation of the founders' intent. Others are the aggregation of administrative authority in government that permits officials to behave arbitrarily, without proper definitions, process, and remedy. An example is the management of information security. The temptation to create a category of information called "sensitive but unclassified" has already created a great deal of confusion and nervousness in the technical community, since the criteria for defining a security breach seem to be created after the fact in each case.

One solution is to recognize the principle that governmental responsibilities should be assigned to the level of government where the information about a threat is located, where the damage will be inflicted, and where the human resources to deal with it must be mobilized. Under the U.S. Constitution, states have quite adequate police powers to address many terrorist threats, if assisted by federal financial, technical, and intelligence resources. If constraints on civil liberties (still consistent with constitutional protections) are adopted more locally, the trade-off of value and cost is more likely to be politically acceptable and less likely to lead to a loss of power in the central government. The national government's role should be to ensure that the states do not go too far in constraining personal freedoms; it should not be the instrument of abuse of those freedoms. Indeed, the observation cited above, that the open societies that tolerate dissent are most vulnerable, clearly implies that any strategy for protection from terror attack must be designed to protect the right of political dissent, not to suppress it in the search for those who might be sympathetic to terrorist objectives. Technology can play a role here too. By reducing the number of attractive targets, decreasing the likelihood of a successful attack, and increasing the resilience of those targets that are attacked, the need for more extreme abuses of civil liberties can also be reduced.

SUMMARY AND CONCLUSIONS

There are seven major points that I would conclude from this discussion.

First, only a far-sighted foreign policy, addressing the roots of terrorism and denying terrorist ideologies a foothold in other societies, can make the United States and its allies safer in the long run.

Second, weapons of mass destruction are potentially devastating, but the most probable threats will be fashioned from the economy itself, as was the case on September 11, 2001. Private property and commercial industry are most often the target of terrorist attacks, and may be providing the weapons for their own destruction. Thus, the federal government must devise both positive and negative incentives for private investments in hardening critical infrastructure and urban targets.

Third, the protection of critical infrastructure must, to the extent possible, be accomplished through a civilian benefits maximization strategy.

Fourth, reducing vulnerabilities in critical infrastructure is a highly complex systems problem; it requires a strategy tested by the most modern systems analytic approaches.

Fifth, since most of the science and technology capability of market economy governments lies outside the security agencies, governments must be able to coordinate and fund a national science and technology strategy.

Sixth, a degree of cooperation between industry, cities, and government unknown in prior experience is required. In particular, local authorities must have an effective voice in setting the technical agenda for equipment for which they are the customer.

Finally, for the protection against terrorism to be sustainable, more than a civilian benefits maximization strategy is required. The negative effects on civil freedoms from increased authority in the central government must be resisted, since the threat of terrorist attack is indefinite and emergency measures may never be relaxed.

2

Terrorist Threats in India

Major General (Retired) Afsir Karim

Terrorism in India takes two forms: one is of domestic origin, the other is terrorism that is sponsored by external agencies. The domestic terrorist threats in India basically arise from separatist tendencies, ethnic and linguistic demands, religious radicalism, socioeconomic deprivation, and, at times, bad governance. Domestic and localized terrorism attains dangerous proportions only when backed by external powers or agencies that provide arms, explosives, and base and training facilities to the insurgents. Transnational jihadi terrorism, sponsored by another country or a religious group to achieve geostrategic objectives, currently poses the main threat to India's national integrity and socioeconomic cohesion. Jihadi terrorism is conspicuous by its absence among Indian Muslims. This suggests that democracy and liberal values inhibit the kind of behavior that leads to jihadi fervor that easily translates into terrorism as a political weapon. Unless the terrorist infrastructure in Pakistan is dismantled, terrorist threats to India and to the entire region, including Afghanistan, will persist, as Pakistan remains the center of gravity for terrorist activities on the subcontinent, though some elements have been relocated to Bangladesh.

Finally, a number of factors facilitate subversion from abroad and sponsored terrorism. These include

- ethnic or religious affinities in border areas or other religious susceptibilities that can be exploited
- suitable terrain where covert operations can be conducted, such as smuggling of weapons by smugglers operating in unguarded coastal areas, mountains, jungles, or vast desert stretches
- cleavages in a society or within separatist groups that allow foreign elements to establish links in order to further terrorism, provide mutual assistance, or exchange information and intelligence
- bad governance and rampant corruption within a state
- contiguity of borders with hostile states
- lack of stability in neighboring countries

- ethnic or religious clusters in densely populated ghettos in large urban centers, where policing is difficult and terrorists and their weapons can be easily concealed

REGIONAL TERRORISM IN INDIA

Pakistan's Inter-Services Intelligence Directorate (ISI) network in India has collaborated with selected disruptive groups in order to encourage regional, ethnic, or religious cleavages with a view to disrupting normal life and undermining confidence in the government. ISI has also established links with crime syndicates in order to facilitate drug trafficking, weapons smuggling, and the distribution of arms and explosives to subversive elements already active in the country. It also has a sophisticated communication network from which it launches cyber attacks, and it gathers intelligence, establishes safe houses and arranges border crossings for covert operations and terrorist activities. Finally, in addition to recruiting and training subversive elements for purposes of sabotage, it has coordinated attacks on India's industrial and economic infrastructure, as well as on special targets such as the Indian Parliament.[16]

A general survey of terrorism and violence-prone regions in India reveals common features that promote terrorism and violence. Outside of urban areas we can divide India into four zones where terrorism has appeared in some form – the northeast, western, southern, and central zones – with the northern state of Jammu and Kashmir (J&K) being viewed independently.

The Northeast Zone

India's northeast states (Assam, Manipur, Meghalaya, Mizoram, Nagaland, and Tripura) constitute a very complex set of diverse cultures, many of them tribal in nature. These states have more than 4,000 kilometers of international borders, and the entire region has been prone to some form of insurgency and terrorism for decades.

In the last 20 years there has been a gradual escalation of the violence in all of the insurgency-prone areas of the northeast. The United Liberation Front of Assam (ULFA) has staged a comeback in Assam. It was able to establish bases in Bhutan out of the Indian security force's reach. Eventually, the Royal Bhutan Army mounted a special operation to evict the ULFA.

The militants formed links with tea estates and with other industries and bought safety. This provided the militant groups with easy and almost unlimited sources of financial help. The top command of the ULFA has well-established links in London, Singapore, Bangkok, and Katmandu. The ISI continues to maintain close links with the ULFA and other militant cadres through its proxies in Bangladesh.

The All Bodo Students Union issued a call for a separate state in November 1998. Despite an agreement between Bodos and non-Bodo tribes in 1993, peace did not return. Neither the Bodos nor the non-Bodo tribes were happy with the arrangements suggested in this accord. As a result, brutal attacks, killings, and ethnic cleansing continue.

[16] On December 13, 2001, the Indian Parliament was attacked by suicide bombers killing 12 people. See: http://news.bbc.co.uk/2/hi/south_asia/1707865.stm.

Insurgency and terrorism in Manipur continues because confrontation between Meities, Nagas, and Kukis results in brutal killings. Different militant groups, however, have varied political aspirations and demands. Therefore, much confusion prevails.

Insurgent-terrorism in Tripura arose following a large influx of immigrants. As a result of this influx, the original tribal population dropped from 93 percent to 29 percent of the overall population between 1947 and 1981, becoming a minority. Ethnic clashes between tribals, Bengalis, and people from Assam continue to provide an impetus to the insurgency and to terrorists in the state.

The movement against outsiders in Meghalaya has become violent. The latest round of terrorist activities showed that fresh consignments of arms and explosives have reached Meghalaya recently.

Insurgencies have continued unabated in the northeast for the last 50 years. The northeast falls along the transit route used to smuggle narcotics from the Golden Triangle of Southeast Asia. This facilitates arms smuggling.

Terrorism has been used as a political weapon whenever movements in the region start losing momentum. It is a factor in the unrest and insurgency in Nagaland, in the Naga-Kuki conflict in Manipur, in tribal violence in Tripura, and in the Bodo and ULFA movements in Assam.

The northeast states have a tenuous connection with the rest of India because of the narrow Siliguri-Jalpaiguri corridor. The region is extremely vulnerable to external influences because it shares extensive international boundaries with Myanmar and Bangladesh and it has diverse, warlike tribal populations that spill over state and international boundaries. The people of this zone have close ethnic religious affiliations with the people of Bangladesh and Myanmar. Movement of insurgents and weapons to and from Bangladesh, Nepal, Bhutan, and Myanmar into this zone can never be fully controlled because of porous borders, difficult terrain, and ethnic affiliations.

The Western Zone

The entire western zone (including the states of Maharashtra, Gujarat, and Rajasthan) has been prone to international terrorism. Maharashtra and Gujarat have had serious communal problems. Mumbai and Ahmedabad have been targets of retaliatory terrorism with the help of jihadi groups based in Pakistan and crime syndicates in the United Arab Emirates. Rajasthan has been a convenient route for arms smuggling and for drug trafficking across the Pakistan-India border because it is not easy for the authorities to patrol such a vast desert area. The communal divide that has been created deliberately in Punjab and Jammu and Kashmir has led to a particularly brutal form of terrorism.

The Southern Zone

This zone includes the states of Andhra Pradesh, Karnataka, Kerala, and Tamil Nadu. Tamil Nadu faces Sri Lanka across the waters of the Gulf of Mannar. The main cross channel traffic is of small boats across the Palk Strait. The heavily forested terrain in western Ghats, Annamalai, Cardamon hills and the Niligiris suits brigands and terrorists. The majority of the people speak Tamil, the language of the Liberation Tigers

of Tamil Eelam (LTTE). Ethnic and linguistic affinities as well as easy access to and from Jaffna enable the LTTE to find safe houses both for terrorists and for arms caches. Random terrorist activities have been frequent in Jaffna. Former Prime Minister Rajiv Gandhi was assassinated in this region with the connivance of the LTTE.

Karnataka provides excellent areas for covert operations of both crime syndicates and subversive groups. LTTE cadres were active here some time ago. Kerala has extensive jungle cover and a long coastline from which traditional trade links have existed with the United Arab Emirates. The coastal Kerala has been a transit area for the smuggling of arms. The population mix and easy access to Gulf money also makes it a popular hideout for terrorists on the run. The southern tip of Kerala faces the Gulf of Mannar, which the LTTE has used for arms smuggling.

The Central Zone

Andhra Pradesh, Orissa and parts of Madhya Pradesh Bihar Jharkhand and Chattisgarh are presently the main areas where armed leftist groups or Naxalite are active. The People's War Group (PWG, now also called People's War) and the Maoist Communist Center (MCC) operate in Bihar and are among the most ruthless killers or terrorists. Other elements have lately stepped up violence in various areas. The PWG has affiliations with crime syndicates for the procurement of arms and is a natural ally of the international terrorist gangs and Maoists of Nepal. The avowed aim of these groups is to fight socioeconomic injustice. They regularly attack the police, officials, and politicians. They make extensive use of improvised explosive devices to attack vehicles. The chief minister of Andhra Pradesh was recently wounded in one such ambush. Remote jungle areas with hilly terrain provide ample cover for the training and operations of Naxalite terrorist groups. Private military groups such as the Ranvir Sena are caste-based armed groups who terrorize other castes by gruesome killing.

Urban Centers

India contains many of the world's largest cities, and some are notorious for terrorist activities. Mumbai, in particular, is well known for criminal-assisted terrorism, mafias, and money laundering activities. Since the Babri Mosque was demolished in 1992, it has become a hotbed of ISI activities. In Mumbai the criminal gangs of Dawood Ibrahim, Chota Rajan, and Arun Gavli receive extensive support and assistance from foreign terrorist groups who provide safe houses for them in Pakistan and Gulf countries.

Mumbai also serves as a base of espionage activities. It is a transit point for the distribution of arms and explosives to subversive elements, drug peddlers and radical communal groups throughout India. Several devastating bomb blasts have occurred in Mumbai since 1992.

Delhi, Calcutta, Hyderabad, Ahmedabad, and at least 30 other densely populated urban areas have active subversive-terrorist cells; Lashkar-e-Taiba (LeT) is also reported to have established terrorist cells is some of hese cities. In the chaotic conditions of

overcrowded cities, it is easy for terrorists to establish arms caches and designate clandestine meeting points near their chosen targets.[17]

Jammu and Kashmir

The situation in the northern state of Jammu and Kashmir deserves special attention. There are a number of reasons for the high incidence of terrorism in this state, including a lack of effective governance and corruption at multiple levels of the administration, ethnic and religious divisions, the inaccessibility of certain areas because of a lack of infrastructure, weak information management and counterpropaganda techniques, and ethnic and religious affiliations with Pakistani-controlled Kashmir.

In J&K, Pakistan's psychological warfare and effective religious indoctrination remains largely unchallenged. It has launched highly trained jihadi-terrorist groups for terrorism, sabotage and attacks on high-security areas, and supplied arms, training, and financial support to domestic terrorist groups. As part of its strategy, Pakistan launched jihadis into Kashmir with the objective of thwarting the Jammu and Kashmir Liberation Front (JKLF), an independence movement launched in Kashmir, and converting it into a religious and pro-Pakistan movement. Pakistan has also used jihadis to wrest Muslim majority areas of Kashmir from India through a combination of political subversion and insurgent-terrorism. Terrorism has been used to intimidate the people and state authorities and make them meekly submit to Pakistani aims, and Pakistan has sought to awaken Islamic fundamentalism in order to assert Islamic identity and obviate any chances of compromise between the people and a secular government. One other strategy has been a campaign of ethnic cleansing designed to force Sikh minorities to leave Muslim majority areas in the state, and to incite communal trouble in Kashmir and in the rest of India. Pakistan's overall goal has been to bring attention to the Kashmir problem to the international level, presenting India as a repressive state that is using military power to suppress a popular uprising in J&K.

The current phase of terrorism poses a threat to the composite culture in Kashmir and to the territorial integrity and unity of India. Influenced by Pakistani extremists, a crucial change has taken place in the religious ethos among the Kashmiri Muslims. They have shifted away from moderate Islam to radicalism. Some religiously based Hindu parties of India are inadvertently helping Pakistan to consolidate its position in J&K by calling for a separate identity and making provocative statements against the Kashmir Muslims. Although Pakistan has not been able to achieve its political objective of wresting J&K from India, it has succeeded in creating anti-India feelings and a Hindu-Muslim divide in a large segment of the population.

To defeat jihadi terrorism, both armed and unarmed, fundamentalists must be defeated in Kashmir. However, even this would not stop cross-border terrorism completely unless Pakistan takes firm steps to dismantle the terrorist infrastructure erected for jihad in Kashmir.

[17] A major terrorist attack took place in December 2005, on the campus of the Indian Institute of Science in the high-tech city of Bangalore, and one eminent Indian scientist was murdered.

SUMMARY

It is important to reiterate that terrorism in India has many sources. There are indigenous movements based upon regional separatist and ethnic movements, and there is an extensive network of externally supported forces. Finally, radial jihadi terrorism among India's large Muslim population is notable by its absence, as democratic politics provides an outlet for the expression of grievances.

3

Discussion of Terrorist Threats in the United States and India and Relevant Science and Technology

B. Raman and Harry Barnes,
Discussion Moderators

In the discussions of the Lewis Branscomb and Afsir Karim papers, three broad themes were explored: (1) the types and trends of terrorist threats, (2) the role of science and technology in countering terrorism, and (3) specific concerns (costs, threat to freedom, and organizational capacity) raised by the need to respond to terrorism.

TYPES AND TRENDS

As for types and trends of terrorism, several Indian commentators noted the differences between present-day terrorism and what preceded it. M.K. Narayanan, expressed the concern that terrorism had become a strategic weapon, and was far more widespread than it had been in the past. He also noted that there was still disagreement over the definition of terrorism; except for United Nations' Security Council Resolution 1373, which provides a certain operational definition, there is neither an agreed theoretical nor doctrinal statement as to the definition of terrorism. The last major effort to define terrorism was at a conference in Sharm-el Sheikh, Egypt, in 1995, and wisely, Narayanan added, people have not tried to hold another such conference.

Narayanan noted four differences between present-day terrorism and that of the past. First, we now have "postmodern" terrorists, able to operate as loosely organized, self-financed networks. Second, religiously oriented terrorist organizations have eclipsed the earlier ideologically motivated and ethnonational terrorists of the past. Third, there is a growing cross-pollination of ideas among terrorists as they become better networked—more so than among the various counterterrorism agencies. Finally, the new recruits to the ranks of terrorism are amazingly sophisticated, many of them with advanced training in science and engineering. Narayanan noted that this could mean that their appetite for acquiring crude nuclear weapons or weapons of mass destruction is growing; before long they could contrive to build a crude nuclear device.

The latter point was also emphasized by B. Raman, who stated that terrorists were becoming increasingly adept in the use of science and technology for their own purposes. They attract a large number of educated people from universities and other educational institutions. In the past there were ideologically oriented organizations such as the Bader-Meinhoff, the Action Directe of France, the Red Army faction, the Red Brigade, and so forth. The people attracted to those terrorist organizations were largely humanities students, rarely were there any science students. We now find that many members of terrorist organizations are science or engineering students and technical professionals, notably Osama bin Laden (himself an engineer) and other members of al Qaeda. One suspect in the Bali bombing held a doctorate in chemistry from a very prestigious British university, and Abu Zubaida, who was supposed to be the third-ranking person in the al Qaeda hierarchy, was an expert in computer technology, and according to some reports, studied computer technology in Pune, India, and then crossed over into Pakistan where he joined al Qaeda.

Raman noted that in Pakistan two scientists went to Kandahar and met Osama bin Laden and the leaders of al Qaeda—it is just as important to study the impact of religious fundamentalism on the scientists who deal with missiles and nuclear explosives as it is to study the impact of fundamentalism on political leaders or the armed forces.

Raman emphasized the ability of terrorists to improvise: they discovered 20 years ago that the Czechoslovakian explosive Semtex was difficult to detect, they used airplanes to deliver deadly attacks, and they used shoes to conceal explosives. The lesson is that we must constantly monitor their thinking; for example, in 1998, after the United States launched cruise missile attacks on the training camps in Afghanistan, groups close to al Qaeda said, "You came and attacked us with your cruise missiles on our territory. We will one day come and attack you on your territory with our cruise missiles." A statement that at the time was not taken seriously, but in retrospect it seems to be significant. Terrorist statements have to be monitored seriously, not dismissed as bombastic. On the other hand, Raman noted the problem of dealing with terrorists who claim to possess a bomb or a grenade on an airplane, but have only dummy weapons. He asked whether the issue of sorting out credible and noncredible threats had been adequately examined, as had the prior problem of preventing scientists in such states as Pakistan from sharing their expertise with terrorists.

Continuing on the theme of the role of the scientifically trained terrorist, S. Gopal noted the difficulty in detecting such people. Hypothetically, this would mean that each state had to develop a database of people working on high-end technology and perhaps exchange this information with others. One possible way to track this threat would be to have proper intelligence on people in every country working on high-end technology. He agreed that this would, of course, impinge upon individual rights and freedoms, particularly if intelligence gathering included asking if such people had problems, if they had been affected by state activities, or if their family was affected in some way. But being forewarned is forearmed. So a good network of intelligence, both human and technology intelligence, is a must to minimize terrorism.

Another Indian participant, Raja Menon, was impressed by the diverse range and objectives of terrorists in the world today; from the eastern branch of the terror network, the Jamma Islamiya, with clearly proclaimed political objectives, to terrorist organizations that may be open to negotiation. On the other hand, Menon noted,

Branscomb was correct when he described a new kind of terrorist group whose actions are largely unpredictable, since their objectives are largely idiosyncratic and obscure. That describes al Qaeda, whose political objectives are obscure, and to the degree we understand them, not really negotiable. This type of terrorism most likely will not end soon. Science and technology might be focused on monitoring the transfer of money, as all of these groups, whether Indonesian, Syrian, Egyptian, Saudi, or others, have in common the need for money.

Suggesting a large-scale international approach, G.R. Srinivasan stated that one goal of terrorism is to create economic loss and disruption, which has happened in India, although not in the United States, except for the massive economic damage inflicted by the September 11, 2001, attack. Srinivasan suggested that the international community might ban the use of terrorism to attack another country's economy. The key is in making states responsible for this, drawing on the analogy with warfare, where the United Nations and international agreements have limited the conduct of war by states. Globalization means that if states exercise their responsibility in preventing terrorism, then it can be stopped.

As for long-term trends, several participants expressed their concerns. Narayanan pointed out that while the appetite for violence was growing, there are no good answers as to why this surge has taken place. Like a hydra-headed monster, terrorist forces keep rising up again and again, both in the developed and in the developing states. How, he rhetorically asked, can we deal with a problem where one day a Tunisian-born al Qaeda terrorist plots a suicide attack on a NATO (North Atlantic Treaty Organization) air base in Belgium, a Humbali in Indonesia carries out attacks all across Southeast Asia, and in Guatemala Bay a U.S. soldier and an airman of Syrian origin are associated with them? The problem is growing more acute for India, with its fast-growing economy; Narayanan urged the scientists and scholars present to identify some concrete answers to a problem that seems to be more acute than at any time in his long experience in dealing with terrorism.

N. Balakrishnan pointed out one difficulty in applying science and technology to the terrorism problem. It was analogous to encryption and decryption, where the cost of encryption is miniscule compared to the cost of decryption. If a terrorist invests $10 on science and technology in a terrorist act, the persons who have to contain it may have to spend thousands or tens of thousands of dollars; therefore, science and technology may favor the terrorist.

Suicide Terrorism

At various points, the group discussed the growing phenomenon of suicide terrorism. Narayanan noted that India has already had at least 60 documented instances of suicide bombings. Unlike the suicide bombers in the Palestinian-Israeli conflict who target public places, many of the targets now are fortified camps, making locations with nuclear fissile material a highly likely target. Additionally, chemical and biological laboratories are increasingly visible targets, as more and more publicity is given to biological warfare and the use of dangerous pathogens. The suicide bomber who does not care whether he or she dies in the process of releasing smallpox or anthrax is going to be a significant threat. According to our estimates, there are almost 15 to 20 persons

volunteering for a suicide mission for every 1 person selected, and if this is true for India, it is equally true for the rest of the world. This is a problem that cannot be ignored. Narayanan noted that this is not just a police problem.

He added that India may yet face a growing problem from its own Muslim population; there have been local aberrations, such as Gujarat, but India has 140 million Muslims, the second-largest population of Muslims anywhere in the world; suicide bombers from one's own state pose a tremendous threat, and even the United States cannot afford to overlook it. Suicide bombers are a concern that requires a great deal of interaction and cooperation between the science and technology community and the agencies responsible for human intelligence. Narayanan noted that India's nuclear deterrent had been based on the belief that people are afraid to die, but this is not how suicide bombers feel.

In a lengthy discussion of the suicide terrorist problem, Branscomb noted that the National Academies' (NAS) Committee on Science and Technology for Countering Terrorism spent some time arguing about the definition of catastrophic terrorism, with some members wanting a kind of mathematical description in terms of deaths and damage. The group decided against this approach, because it concluded that from a terror point of view, probably the most devastating attack would be if once a week someone blew up a daycare center full of children. And if that persisted in different cities over a period of time, the American people would become extremely distraught. Nevertheless, because we were writing about science and technology, we did not quite see how it would be a powerful tool for dealing with a suicide bomber, at least of the type that is seen in the Palestinian-Israeli conflict. Therefore, *Making the Nation Safer*[18] limited itself to the problem of catastrophic terrorism in which thousands of people were killed and billions of dollars of damage was done, even if a series of small attacks over time would have at least as big a political and social effect on a country as a single, more devastating attack.

Gopal intervened to note that 100 percent defense against suicide bombers does not exist, although fissile material can be kept out of their hands. For example, on the local level, we can create a restricted perimeter around a possible target to mitigate the damage from an attack such as a truck bomb.

Richard Garwin offered his views on the problem of suicide bombers. He noted that the intersection between those who are willing to die and those who are willing to be terrorists has been very small in the past, as is the number of those who are capable of fitting themselves with powerful weapons. Yet, he warned, this is rapidly changing, as more and more people become disaffected. Here, modern technology adds to the problem. There are not only terrorist networks, but the Internet makes it possible for people to learn techniques of destruction so that individuals no longer need to invent them. In addition, there are terrorist supply networks, which recruit and provide those willing to die with the required technology. Garwin noted that a terrorist does not have to assemble his or her own makeshift explosive belt anymore, as these are now being perfected and supplied. Fortunately, this is a point of vulnerability for terrorists, as the police arrest those who are in the business of making such weapons.

---

[18] National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, D.C. The report is available in PDF format at *http://books.nap.edu/hml/stct/index.html*.

Ironically, Garwin noted, the greater the range of weapons in the hands of terrorists, the less they need to rely upon suicide bombers. If the weapon has a radius of destruction of a kilometer, that is, an actual nuclear explosive, it is all too easy to release it anywhere within that region and then for the person who has done it to leave. But, he pointed out, it is true that suicide bombers can have a great advantage in penetrating a nuclear plant, for example, or in attacking a chemical plant, with results comparable to or more serious than those at Bhopal, because a nonsuicide attack would require the placement of an explosive at a particular point and the safe departure of the perpetrator.

THE ROLE OF SCIENCE AND TECHNOLOGY

Narayanan argued that science and technology will have to play a much greater role in the future than in the past because of the extraordinary reach and the tremendous potential for destruction caused by terrorism; far from being a tactical weapon, terrorism has become a strategic weapon of those seeking mass destruction. Raman suggested that "counter science and technology"—how the state uses technology to prevent terrorists from using science and technology assets maliciously—is as important as how the state uses science and technology to respond to terrorist acts.

From Raman's perspective the most important contribution of science and technology to terrorism prevention is in respect to communications. Wherever interception of communications has been effective, states have been able to prevent acts of terrorism. This is evident in the tactical success of the United States against al Qaeda in Afghanistan and Pakistan; however, it was unable to score similar successes in the cases of the Taliban or the resistance fighters and terrorists in Iraq. al Qaeda used highly skilled experts for its communications, but went through the Internet, providing an opportunity to intercept messages, while the Taliban lacked such expertise and did not use this technology, thus preventing the interception of messages. In Iraq the resistance does not use telephones, wireless communication, or the Internet; they do not even call themselves by name. Thus, the more that terrorists use science and technology the more vulnerable they are to detection and neutralization by the state, and the less they use technology, the more difficult it is for the state to detect and neutralize them. Raman noted that the dilemma for policy makers is that by denying terrorists modern means of communication, we may also hinder our own ability to detect and neutralize them.

Kumar Patel raised the issue of the cost-effectiveness of using technology to defeat or detect terrorists. He noted that it is not very difficult to do a simple calculation of the additional costs and time that go into screening people at airports. Some 2 billion people take airline flights every year in the United States. If we calculate the effects of the accumulated lost productive work time, we can easily determine the cost of added airport security. It is not large, but this happens at every single step. There is a general belief that if only we spent enough money, we could make ourselves much safer, but in Patel's view, this is like buying insurance. Someday, insurance payments may exceed current income, and at that point you will know that you cannot buy any more insurance. The point is, How can we convey through science and technology and cost-effectiveness calculations that at some point we may have to accept a certain level of disruption in society because we cannot afford to be 100 percent safe?

This was a point echoed by Gopal, who doubted whether science and technology would ever provide a 100 percent solution to the challenges of terrorism, and he noted that in one recent instance, an attempt on the life of an Indian chief minister was not defeated by high-tech jammers, but the strength of his vehicle, as the explosives were set off by a wired mechanism.

There was a brief exchange over electromagnetic pulse (EMP) devices and radiological attacks. S. Rajagopal noted that it could be used to seriously damage power lines and connected system equipment and components. Branscomb noted that something the size of a suitcase can easily be made that would have the effect of shutting down and perhaps damaging computers within a city block; this could be used against an emergency operations center, for example. Branscomb believed some public knowledge about this topic would be beneficial to security rather than injurious to it.

Branscomb also responded to Rajagopal's query about modeling of cleanup and decontamination from a radiological attack. He noted that some attention was being given to cleanup and decontamination, probably not as much as it deserves, because the principal effect of a radiological attack is likely to be denial of access to the contaminated space. If people leave fairly quickly they are not likely to be physically harmed, but if they cannot return, there would be economic consequences and social disruption. That, Branscomb concluded, deserved a lot more attention than it has been given, even though large amounts of money (much of it for lawyers) had already been spent studying and carrying out decontamination projects from industrial and government nuclear sites.

SPECIFIC CONCERNS

Indicators

Raman urged the development of terrorism indicators, analogous to the way intelligence and counterintelligence agencies have developed lists of war indicators. The report of the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, indicates that there were disparate pieces of information indicating some suspicious activity, but in retrospect, if all those pieces of information had been put together there might have been a successful forecast of a terrorist attack. There should be a group of people, including scientists and terrorism experts, who could prepare a list of terrorism indicators and share these with government agencies.

Networking and Organizational Responses

The discussion of the Branscomb and Karim papers also led to an extended dialogue on the importance of networking counterterrorist operations and improving the response of organizations. In response to a question, Branscomb noted that the issue of effective networks for acquiring and creating information and for supporting decisions was a very high priority issue of the NAS committee which published, *Making the Nation Safer*. While there is a lot of experience with complex systems and networks in other environments, some are rather special, and involve the military in some cases, and commercial applications in others. The problem is that the networks needed for

counterterrorism must be very inexpensive. The United States could probably afford them, but networks must also operate in a disrupted environment, something for which most commercial systems are not designed. Branscomb noted that this is a promising area for collaboration between the United States and India.

Roddam Narasimha noted that terrorists in India depend very much on networks, sometimes very tightly knit and very closely organized, and sometimes a little more loosely so. These networks have involved state and nonstate actors and operators, as is clear with Pakistan's involvement. In Jammu and Kashmir, networks have also involved religion, crime, social and ethnic conflict, and technology.

Narayanan urged that even more powerful counterterrorism networks be established both within states experiencing terrorism and between those with populations of different religious persuasions and diverse societies. Strong networks between different countries have been necessary to control drug traffic, the flow of funds, religious and social propaganda and misinformation, and to exchange and analyze data and information as well as to exchange databases and ensure the universality of extradition treaties and mechanisms. There may be some movement in this direction, he conceded, but he doubted whether these networks were sufficiently strong—especially since Narayanan felt that the terrorists had more powerful and effective networks than states.

Narayanan did agree with Branscomb that one powerful aspect of technology is handling information. However, the generation, fusion, mining, and secure transmission of information in real time to intended recipients actually present scientific and technological problems, which Naryanan thought was fruitful territory for future Indian and U.S. cooperation.

Civil Liberties

In response to a question from Harry Barnes about the impact of the struggle against terrorism on civil liberties, Branscomb noted that the U.S. President and many political leaders constantly refer to our present state as "a war on terrorism." This is a war in a symbolic sense; the U.S. has talked about wars on poverty, wars on drugs, wars on HIV/AIDS, wars on cancer—none of these were wars in a traditional sense except the notion of a dedicated high priority for government action. But, Branscomb pointed out, President George W. Bush uses this word in combination with what is a real war in Iraq, implying that the terrorism problem is a national emergency on the scale of previous world wars. In Branscomb's view, however, terrorism is an urgent security threat, but is not a war. The terrorist threat will not go away. Terrorists are not going to win; governments are not going to win; nobody is going to win. Vulnerabilities will continue, new threats will arise in the future, but the survival of the nation is not at stake, however greatly the threat of terrorist attacks upsets the public and its government. That being so, the steps that may be necessary to improve the capabilities of intelligence services and the police must be measures that can be sustained in a democracy indefinitely. Therefore, the analogy of the United States incarcerating its citizens who were ethnic Japanese during World War II is not a good analogy to contemporary actions. Japanese

imprisonment was justified at the time on the grounds that World War II would have a finite duration. We would win or lose. Losing was unacceptable, and therefore winning had to be accomplished. It could not take more than a few years, and therefore we could suspend constitutional rights for this emergency.

Branscomb warned that if we take similar actions today, we are in deep trouble, because the suspension will continue indefinitely. We will no longer have a democracy, and we might as well yield to the terrorists. He expressed his belief that the civil liberties issue had to be addressed with great subtlety and care, although he did not deny that the police and intelligence services need more ability to perform their duties.

Severe Acute Respiratory Syndrome and Grid Threats

The group also discussed two events that might hold lessons for dealing with possible future terrorist attacks: the Severe Acute Respiratory Syndrome (SARS) epidemic and the collapse of the power grid across about one-third of the United States in 2003.

Lawrence Papay discussed the grid crisis, echoing a comment by Branscomb that if this had been a terrorist attack, the system would not have been restored quickly. This issue was discussed also in the workshop session on infrastructure protection, but Papay did remark that it showed the actual fragility of the grid. While the National Academy of Engineering said the electric power system in the United States was the greatest engineering achievement of the twentieth century, the blackout showed the vulnerability of the electric power grid, and how susceptible it is to a terrorist attack.

Branscomb thought that the SARS episode was a test case of how we might respond to a biological attack. The appropriate response to SARS was a fourteenth-century approach, namely, take all the people who have been anywhere near the affected person and quarantine them in their homes, and then hope for vaccines once the disease has been identified. That approach proved successful in the SARS outbreak, and it demonstrates the absolute necessity of revitalizing the public health service at the local level in the United States. Years ago if a child in the family got measles, a public health officer appeared immediately at the home, nailed a yellow sign to the front door of the house forbidding anyone to go in or go out until those affected recovered so that the measles would not spread to others. That is exactly the strategy required for SARS. It is a necessary but not sufficient strategy.

The possible causes of a public health crisis are not limited to SARS. Four naturally occurring viruses struck humans in 2003, all of which fatally affected a percentage of patients and required quarantine. Garwin noted that, in a way, the SARS outbreak was very similar to the collapse of the electrical grid, and we were extremely lucky that SARS had the characteristics that it did and that the symptoms were apparent before it was contagious, leading to the possibility of effective quarantine.

As to the possibility of terrorism, Garwin pointed out that foot-and-mouth disease emerged in Taiwan a few years ago, and there was a question as to whether that was an act of terrorism or, for that matter, a China-sponsored introduction. There, too, it appeared in one place and spread in the usual fashion from the place of introduction. It could be that a terrorist might be generous, and not want to inflict maximum damage, but a terrorist might well introduce the disease in multiple places at the same time. The

forensic investigation might produce evidence of a terrorist attack, but perhaps it would not; identifying the nature of an outbreak (terrorist or not) is an important problem, but our larger task is to protect, whether or not we know it is terrorism.

Impact on Policy

Both U.S. and Indian workshop participants briefly discussed the relationship of science and technology to policy formation. Branscomb noted that *Making the Nation Safer* had a strong impact because it was released one week after President George W. Bush changed his policy and decided to seek congressional approval for the creation of the Department of Homeland Security (DHS). The report's recommendation that the new department include an undersecretary of the Department for Science and Technology was accepted; this office has responsibility for all science and technology policy at DHS. Additionally, the major recommendation that science and technology should be taken seriously as part of the national counterterrorism strategy was accepted—however it remains to be implemented. Finally, what Branscomb called the most important specific proposal of *Making the Nation Safer* was the creation of a Homeland Security Institute (HSI). This was to be a federally funded, nongovernmental but dedicated organization with very high level systems engineering and modeling expertise and decision-making skills to address these complex problems. The primary tasks of the organization would be vulnerability assessments, priority setting, and analysis of proposed actions. A well-qualified systems analysis contractor, the ANSER Corporation, was selected to create and operate the HSI, but it has not been able to operate at a broad level in DHS, nor get the authority it needs to do the job envisioned in the NAS study.

There was also a discussion (mostly among U.S. participants) as to the role of local and state governments in implementing a strategy to contain or prevent terrorism, and the relationship of local governments to the federal government bureaucracies. Branscomb noted that there remains much to be done regarding how to decentralize, down to the community level, the ability to detect the likelihood that persons in the community might pose a threat. If that is done at the national level, in a large country such as India or the United States, it would lack subtlety. Of course, there must be a national police effort, because it is at this point that the international intelligence community would be important. He added that some of the proposals from the Department of Justice would have been unacceptable at the local level and therefore not likely to be implemented (for example, encouraging commercial services that deliver mail or boxes or newspapers to peek inside the door of the house when they deliver and look for suspicious activity). This is very close to asking children to tell on their parents, and is intolerable in a society where liberalism is part of the definition of freedom.

Moving from issues surrounding the scope and threat of terrorism, and means to combat it, Rose Gottemoeller addressed the problem of developing a "customer base" for the new technologies being produced to counter terrorism, pointing out that there was no clarity as to the strategy by which local and state officials might be equipped with the relevant technology. Municipalities, she argued, did not have the resources to buy the technologies, the sensor systems and so forth, that the Department of Energy labs were developing. Branscomb responded that there was also no industrial base for the production of relevant technologies, and state governments were in red ink at the

moment. Ultimately, federal funding will be necessary, but he asked: Will the systems deployed be effective? His answer was that this will depend on whether or not the problem is looked at comprehensively, which was one of the tasks to be undertaken by the Homeland Security Institute. It was intended to be a decision support organization to convince the secretary of the Department of Homeland Security and other senior officials to look at the deployment of these technical fixes in the context of a realistic and comprehensive analysis, including the likelihood that terrorists will become more sophisticated in their attacks. Branscomb estimated that the United States would go through a period of several years in which the money available will be used to purchase whatever is offered by the most politically persuasive vendor, and it will take a few years to find out that it does not work. This was a point also made by an Indian participant, Gopal, who noted that there was likely to be tension between antiterrorist cooperations and commercial interests. The classic example he cited was the 1972 Biological and Toxic Weapons Convention (BWC), which is still hampered because of the conflict between the need for inspections of facilities and the resistance of the biotechnology and pharmaceutical companies.

The session ended with some additional remarks by Raman on the dilemma of dealing with contemporary terrorists. He noted that "classical" terrorists had political gains in mind and did not really want to kill people, but did so only to obtain favorable treatment for their cause. Contemporary terrorists do not care about that, Raman noted; they want to destroy the opponent. The dilemma is that these people will not simply assert that they have a weapon and that they will set it off unless their demands are met; there may well be a weapon that will be detonated without any warning, and this will be the first time we know of it.

4

Information Technology and Communications Security in India*

N. Balakrishnan

The foundation of the information and communication technology (ICT) revolution was laid in the seventeenth century when Gottfried von Leibniz invented the Step-Reckoner in 1671.[19] The Step-Reckoner is a device that can add, subtract, divide, multiply, and evaluate square roots. His invention provided invaluable support for the binary system and marked the beginning of desktop computers. Leibniz asserted that excellent men should not lose hours like slaves in the labor of calculations, which could safely be relegated to anyone else, if machines were used. This premise is relevant to the entire populace, and can be applied to scientists or terrorists.

The information security perspective differs from country to country. Developed countries are concerned with managing and operating nuclear power plants, dams, power grids, air traffic control systems (ATC), financial institutions, and disaster recovery. For developed and developing countries, information technology (IT) is both a weapon and a target.

Capital spending on IT is predicted to increase. IT will soon become a very significant component of the economy. Most countries are predicting that more than half of the economy will be directly driven or indirectly controlled by IT. Economists have found that the percentage of Gross Domestic Product (GDP) spent on ICT can be used to distinguish between developed, transitioning, and underdeveloped countries. The economies of countries that are gradually moving toward becoming developed or moving toward the transition stage will critically depend on IT.

The Internet is not pivotal nor is its functioning critical to Indian society as yet. Nonetheless, information technology is vital to the country's economic security.

[19]The author would like to thank Professor Roddam Narasimha for helping to shape this paper, and gratefully acknowledges the work of his students Meera Sarma and Madhavi Ganapathiraju.

*Editor's note: Since this paper was originally presented in January 2004, many changes have occurred in the fields of information technology and communications security in India. This paper was based on information available to the author at the time.

Software exports have grown in recent years, and ICT has markedly increased as a percentage of GDP. Thus, IT is crucial to our economic security.

ICT forms a growing percentage of GDP of developed economies, a slightly lower percentage of GDP in emerging economies such as India, China, and Korea, and only a negligible portion of GDP in less-developed nations. With the trend seen in the growth of ICT in India as a percentage of GDP, it is likely to match the rate of developed nations. It is only natural to believe that the Indian economy will become more and more dominated by ICT growth.

The effectiveness of ICT in Indian society is quite visible, and we see that economic thieves are increasingly relying on computers and computer databases. In this regard, disk forensics[20] and the laws controlling them are an issue. People who misappropriate funds and launder money maintain all their accounts on computers. Technology is increasingly utilized to trap politicians and political and business opponents. People involved in illegal activities such as betting, economic crimes, and terrorism make use of cellular phones and other technological advancements. Unlike what is witnessed in developed countries, attacks on national networks and the national infrastructure in India are more likely to be politically motivated than motivated by economic gain.

Observation of Internet traffic and intrusion attempts by hackers over a period of time suggests that script kiddies[21] are hacking into some of our networks in order to use the bandwidth to launch attacks on others. Script kiddies are also active participants in chat relays, the cauldron for the formation of hacker groups. The expression of anti-Indian sentiments over the Internet is a spillover of this. This is also made easier by the poor maintenance of some Indian Web sites.

In an effort to improve awareness in the country, the first Indian Computer Emergency Response Team (CERT-In) was launched recently. However, we are still faced with the absence of any serious intrusion detection sensors and few or no intrusion prevention methods and policies in India. With the lack of rules and regulations regarding spam, India could have the largest number of spam mails and the most virus-prone computers in the world. This signifies a need for a national agenda to assist the creation of antispamming laws and best practices for Web sites. If such preventive measures were put into practice, most of our security issues would be solved.

Another important aspect is the advancement of technology and the potential for misuse of that technology. Countries such as India and China could use this as a vehicle for their economic development. Processor technology has already become a nanotechnology. Soon we will witness the convergence of silicon technology with nanotechnology and biotechnology, which will be far more disruptive than ICT. It is also predicted that ICT, biotechnologies, and nanotechnologies together could be more perilous than ICT alone. In the future, IT will be one of several critical factors for the economic security of countries like India.

Storage technology has also demonstrated some remarkable changes. On small form-factor disks, it is possible to store 250 gigabytes (GBytes) today. In 10 years the number of gigabytes on a disc has grown 1,000-fold. There has been an equally

[20] Disk forensics is the science of extracting forensic information from hard disk images.

[21] Script kiddies are relatively unsophisticated computer hackers that look for vulnerabilities in programs through the Internet without understanding those vulnerabilities uncovered by others.

astonishing growth in bandwidth. Seen collectively, the richness and the reach of information are exploding exponentially.

The paradigm shift in Internet traffic is another noteworthy aspect. Until very recently, much of the traffic on the Internet was voice traffic, now data or Internet protocol (IP) traffic has caught up with voice or analog traffic. Currently, the construction of data infrastructure is outpacing voice three to one. With the advent of voice-over-Internet-protocol (VOIP), countries like India will not be far behind. This is a central issue that may create serious problems in the arena of information security in the future.

The major challenge in the area of communication technology is the conflict between connection-oriented and connection-less circuits. Another concern is the seamless integration of broadcast, unicast, and multicast in the midst of growing security concerns. One of the dominant questions about the future of communications is whether there will be wireless and optics alone, or something else beyond fiber technology.

It is most likely that very soon mobile phones will exceed the number of fixed phones. Additionally, they will offer specialized services (that is, calendar, address book, e-mail, and Internet access). The mushrooming growth of mobile phone-like access devices that enable mobility will present a key hurdle in monitoring cyberspace. These devices are small, and determining the location of users may be difficult. The extent of miniaturization is so substantial that in a few years cellular phones will be wearable and will functionally replace many smart devices. The convergences of multiple devices into single devices will, unfortunately, have dire consequences in the sphere of information security.

Digital convergence has led to the creation of smart devices. Behind such digital convergence is the drive toward material convergence and natural interfaces.

The various dimensions of the wireless information society are

- human interface that makes technology transparent
- virtual presence that makes distance transparent
- seamless solutions that make systems transparent

In the upcoming era of virtual presence, the creation of global innovation networks will become possible. These will be virtual communities where ideas, information, and knowledge circulate and collide freely. Together, communication and the technology of computers give life to the concept of information for anyone, at anytime and anyplace.

TECHNOLOGY FOLLOWS THE LAW OF ACCELERATING RETURNS

There is a paradigm shift in the world of computers and communications from supercomputers to smaller microprocessors; in other words, small fish eat big fish. Companies like Cray, Wang, and others have been bought out by smaller companies. Some of them have actually disappeared. Processors could be holographic or have speech input and output with automatic speech recognition and speech synthesis, as well as multilingual and terabit connectivity at a personal computer. In the future, browsers

will be the only medium of communication. They will be active with voice, video, and language, and will be independent. Mobility and small form-factor devices such as palm devices, personal digital assistants, and tablets will be the devices of the future.

Now we can also see the convergence of silicon electronics and photonics. Further, the convergence of biological sciences and nanosciences may make the cyborg a reality. Such technologies may also fall into the hands of antisocial elements. Indeed, computers are gradually moving from thinking machines to spiritual machines. By 2019 a $1,000 computer could have the capability of the human mind.

THE ROLE OF INFORMATION TECHNOLOGY IN THE INDIAN ECONOMY AND THE NEED FOR INFORMATION SECURITY

In India, information technology is going to be a critical factor that has to be protected rather than used as a weapon. Billions of dollars come from IT directly, and the IT market is growing exponentially. Hence, IT—not just the IT infrastructure per se, but also the other components of IT—is extremely critical to the Indian economy. Protecting India's capability for IT expansion is more critical than protecting the critical infrastructure.

In 2002, the vast majority of India's exports were sent to the United States and Europe. Given this, uninterrupted communication between these parts of the world is critical to the Indian economy. For India, IT has also been an excellent economic contributor, leading directly and indirectly to the creation of new jobs and foreign direct investment. Appropriate protection for IT in India should not be limited to just infrastructure, but rather it should be a unique area of comprehensive activity.

Information technology is a critical component of the Indian economy. Knowledge is the wealth of a nation. It is thoroughly interwoven by networks and is often stored on computers as codes, data, and network flow. In the world of digital information, movement of data across a network is essential to the creation of wealth—the digital economy. Hence, physical and economic security is linked to information security. Information security is decisive to India because it is strongly connected to economic security.

E-commerce, supply-chain management, workforce optimization and e-learning are critical enablers of e-business. These critical components will drive requirements, and are linked to economic security. In other words, security is a critical enabler for e-business. In order to achieve security, in-depth defense, which extends beyond classic perimeter controls such as firewalls, is a necessity. Multiple cohesive security components such as intrusion detection appliances and specialized virtual private network (VPN) gateways will have to be used. Security will also have to be integrated into the e-business infrastructure, particularly into enabling networking devices. As security is probabilistic and each security component can either harm or help, a comprehensive blueprint specifying design, operation, and management practices is also required.

There is an explosion occurring in e-business as organizations move to rapidly take advantage of today's Internet economy. As organizations move to use the Internet

and e-business to gain a competitive advantage, they inherently open themselves to new security risks. These risks are significant, and organizations that wish to thrive in the Internet age need to address them.

A dichotomy exists. There is an urge to share information, and at the same time, there is an urge to protect invaluable information. There is a growing need for systems to be open as well as secure. It is predicted that the Internet will become so mission-critical in India that people would rely on it just as much as they rely on the telephone. The Internet is gradually absorbing the phone system, VOIP, entertainment, and digital radio. People will expect high levels of reliability and security from such Indian firms as Telco.

WHY IS THE INTERNET AN EASY TARGET?

The Internet environment today is dynamic, crosses jurisdictional boundaries, and is witnessing an explosion in government, commercial, and consumer use. It continually incorporates new technology but lacks central administrative control. To understand the environment in which incident handlers work, it is necessary to understand that the Internet is global and has no central authority. The Internet started as a research project. It was a small community of researchers who knew and trusted one another. Security was not a primary consideration in the design of Internet protocols. Today, however, any problem that occurs in one part of the world can spread to any part of the world like a virus. Its bandwidth is expanding from dial-up networks. Furthermore, the local area network (LAN) and the wide area network (WAN) have merged, yielding what seems like a single seamless integration of networks. Thus, in addition to the challenge of identifying solutions to protect the current network, a whole new network that looks like one single network has emerged.

Some of the major weaknesses of the Internet are the presence of an ad hoc collection of transmission control protocol/Internet protocol (TCP/IP) interconnections, the absence of a central authority, the lack of central knowledge of connections, poor packet billing, the lack of integration of core equipment in helping law enforcement, and the presence of large perimeters that are difficult to control. Hence, the Internet has become an easy target for individuals and groups intent on doing harm. Since the growth of the Internet has been exponential, it has many hundreds of thousands of vulnerable systems connected to it—all of which are potential gateways or targets for intruders. All are built on an (ultimately) insecure foundation and based on a culture of trust. The Internet itself has become an infrastructure, like the telecommunications or utility services.

Furthermore, the complexity and administration of computer and network infrastructures make it even more difficult to properly manage the security of computer and network resources. As a result, many more computer security events or incidents are occurring. One of the most basic premises is that with the right funding and sufficient time, any network could be broken into. People who try to compromise networks do not have any budgets. They possess blank checks.

DIFFERENT WAYS TO ATTACK

Concerted attacks could be mounted by a combination of agents such as Trojan horses, worms, spies, moles, sleepers, controllers, and couriers. Intentional or unintentional insider attacks are also possible. Denial of service, distributed denial of service, catastrophic denial of service, and social engineering are other types of attacks. In India, very often attacks, such as denial of distributed service or catastrophic denial of service, are absent because the country's backbone bandwidth is not significant.

In this regard there are three components of information warfare—defensive, offensive, and monitoring. The defensive component comprises firewalls, encryption, and secure protocols. The offensive component comprises sniffers, scanners, denial-of-service attacks, viruses, and hardware and software bugs. The monitoring component consists of traffic analyzers, intrusion detection systems, international communication interception, communications intelligence, and passive detection. The monitoring component is extremely important, and many institutions today are collaborating to devise systems that monitor and conduct preventive analyses of attacks.

There are many possible situations presented in the world of information warfare. None of them are possible in India. Nations that are most advanced in networking are also the most vulnerable. A sudden power blackout, nuclear station malfunctions, random changes in airline and railway reservations, or automated teller machines randomly crediting are highly unlikely scenarios in India, particularly because these cannot be attacked through wires. India's telecom network (which is not connected to the Internet), air traffic control systems, commercial banks, and airline reservations are less vulnerable and most of the vulnerabilities are not life threatening.

In most countries, individuals, enterprises, and governments are vulnerable to attacks, but in India the Internet is predominantly used for business-to-consumer activities (rather than business-to-business activities). Given the relative vulnerability of the systems and importance of the targets, it seems likely that, were insider attacks to occur, government information systems and financial information systems would be most affected.

The main problem with ICT is that networks are neither limited by range nor by speed. This means that because of the speed at which information moves, when a network is used in an attack, damage can be extensive and lethal.

INFORMATION LIFETIME

Key players in a networked information society are individuals, enterprises, and the government. These players interact with each other for e-commerce, information exchange, and information dissemination. The economic value of information varies, as does its privacy requirements and the time during which it will require protection. For example, electronic fund transfers require short-term security, as the data is dynamic. In contrast, a company's strategic plans require security for several years. A proprietary product or software would require protection for decades. Personal information, such as medical records and confidential assessments, requires a lifetime of protection.

India has witnessed the communications revolution in different ways. Weapons used could be just words or pictures. India, therefore, is very vulnerable because manipulative information very quickly creates panic.

Information Warfare

Information warfare is the use of information to achieve national objectives. This is done by actions to deny, exploit, corrupt, or destroy the enemy's information and its functions, while protecting the state against those actions, and exploiting the state's own military information functions. Cyberterrorism is a type of information warfare. Future wars are most likely to be fought in this theater. Information warfare affects the economy, commerce, and all of society.

In the field of information warfare, software is the soldier. KNOWBAT, a software spy; daemon sniffer, software that records commands and reports on query; viruses; and trap doors are examples of such soldiers. Computers and networks are also soldiers in information warfare. In India a virus on a chip, electromagnetic pulse (EMP) attacks, EMP-triggered hardware, and biological organisms that eat chips are methods of attack gradually becoming more probable.

Hence, waging information warfare is cheap. There are abundant opportunities to manipulate perception in cyberspace. It is possible to commit virtual fabrication, deception, and propaganda, as no nation has any sovereignty over cyberspace.

The amount of technical knowledge required to be a successful hacker has dropped dramatically. Hacking that required a Ph.D. in computer science in the 1980s can be done today by a school student. The amount of potential damage has also been exponentially increasing, so much so that even a school student could bring down the world's network. Hackers love making the news, and often do, but threats to corporate resources are everywhere. As networks become more sophisticated, so do the tools that hackers use, and today they come with a user manual. This obviously means that instead of a few, brilliant hackers threatening networks, there are many more people of average intelligence and education who can, and do, cause trouble. It is more important than ever to make sure that networks are secure.

PROFILING THE ATTACKER AND ATTACKS VS. PROFILING NETWORKS

With regard to profiling attacks and understanding attacker capabilities, a good research organization can manage to control the attackers' combined capability. A profile of the top defacers worldwide indicates that the Silver Lords, an international group that works in Indonesia and many other places, have caused extensive damage. Such group attacks have been analyzed. Rather than profiling the workings of the networks, profiles of the attackers have been created.

The popular methods of attacks are very informative. Many attacks have been due to configuration and administration mistakes. In many cases, vulnerabilities were known in advance and had been reported in CERT-In and other places, but system administrators had not corrected them. In other words, numerous attacks could have been prevented by being careful or by employing intelligent operating systems and self-healing

networks. Social engineering also accounts for a small percent of the attacks. Undisclosed vulnerability is a factor in a few attacks. If one linearly predicts that the number of attacks is also related to the losses incurred, a large number of the attacks could have been contained if we understood how to work cooperatively.

Hacker Groups

Key individuals working in popular Pakistani-based defacer groups and using Windows are GForce, Moron, and Nightman. World's Fantabulous Defacers (WFD), the Silver Lords, and the Pakistan Hackers Club (PHC) are other groups. The newly formed group Federal Bureau of Hackers (FBH) was quiet for awhile, then on August 14, 2003, it did a mass defacement of sites. The FBH has also written an exploit code. Of all the groups it has a slightly better technical capability.

Pakistani-based groups have largely defaced Indian sites. The Anti-India Crew (AIC) and the GForce defaced many sites. The Silver Lords and WFD also defaced many sites. The Bugs have defaced a few as well. The entire logistical operations of the defacements have been analyzed and mapped. AIC appears to have attacked .com sites and .in sites in equal numbers but did not attack .net, .org, and .edu sites. Many of the Indian sites that end with .com are located in the United States. They have been attacked, but not the sites in India. In information warfare, protecting the Indian border is not going to be a great help.

The same sites have been defaced repeatedly. This is popularly known as *redefacement*. For example, the site of the Regional Research Laboratory in Bhubaneshwar has been redefaced. Gforce is one of the groups that has launched extensive attacks against India. Its operating system (OS) attacks are mostly on Linux. It has very little capability to hack other operating systems. It uses e-mail and file encryptions, rootkits, sniffers, and other methods. It loads the sniffers onto one of the machines, procures the password, and obtains access to the machine.

Hacker Psychology

Observation of attacker capabilities reveals that the majority of attacks could have been done by anyone, fewer required moderate capabilities, and a small percent required higher capabilities. Regarding the level of administrative experience needed by a hacker group to deface Web sites, it is evident that most attacks are common-knowledge attacks. There are very few attacker groups or individuals capable of launching intellectual attacks that require extensive premeditation.

The same group psychology that is used for understanding the development of open software by a heterogeneous mass of people who have not met, or for developing Linux, works for the formation of hacker groups. No credits are given; no brand names are mentioned. However, hacker groups still indulge in defacements.

Certain groups have expertise in compromising certain types of operating systems. For example, GForce has attacked Linux and Solaris operating systems. WFT, on the other hand, has expertise on Windows. The Silver Lords has a combined capability that allows it to compromise Windows and Linux.

A fused analysis, called a science, technology, and psychology analysis, was

conducted to profile the attacks. The aim was to find answers to questions such as, who are these attackers, what are their capabilities, and what should be our capabilities to control them, contain them, or prevent them? Unlike in the United States, attacks in India are predominantly Web-based defacements. These are not the type of attacks by which people have obtained the root password or have gained access to economically sensitive information.

There are three types of Web defacements. Many domains host what are called hosting institutions or host service providers, which host many Web sites. Once the root of the host is compromised, all the Web pages hosted on the sites can be defaced. This is known as mass defacement. There is also re-defacement, the act of defacing an already defaced site. As noted earlier, re-defacing domains is probably the most dismal act that can be committed in the script kiddie world. The All India Institute of Medical Sciences Web site was redefaced. Special defacements are more critical and may have an economic impact. Such defacements would include sites maintained by the government, security agencies, or credit card companies.

Monthly statistics suggest that there are many attacker groups. In recent years, the number of attackers increased, as did the number of defacements and mass defacements. These increases also correspond to India opening up a little more during this time and acquiring more bandwidth for international connectivity. The trends absolutely correlate. The number of defaced sites is also becoming correlated with this increase. Observing the Indian sites that are being defaced, it is clear that their number is growing. Interestingly, the sites that are located outside of the country but are owned by India have been targeted rather than the Indian sites located within the country. This is also related to the access bandwidth.

A thorough analysis of defacements was made in order to find out whether there are political triggers that have been causing fluctuations in defacements. An examination of the country domain defacements indicates that the number of Indian domain defacements is growing.

A closer look at the motives for defacements indicates that the primary reason given for more than about half of the attacks was "just for fun," or "I want to be the best defacer as a challenger, as a patriot." Political reasons accounted for about one-tenth of the just-for-fun attacks. Revenge against a particular Web site was a motive in very few cases.

The next step was to look at a large number of randomly-selected attacks (out of 10,000 attacks, a random sample of 160 was taken), analyze them, and sort them into various groups. The patterns of attacks are similar to the worldwide trend. In other words, out of 10,000 attacks, a random sample of 160 was taken.

The Indian attacks were separated from the total number of attacks and analyzed, then put into various groups again. The number of "just-for-fun" attacks was very small. The number of attacks motivated by "ethnic hate and nationalism" was higher. The number of "political interest and political ideology" attacks on India surpass economic attacks. In other words, attacks on Indian sites are not carried out by organized criminals, but rather by people who want to convey a political message. In this respect, India is completely different from any of the nations of the developed world.

The number of Internet hosts has been increasing in India, which could create future problems. At the same time, the number of Internet servers has been decreasing—

there are many sites that are closing down—and the number of Internet users has been growing. Corporations are aggregating their sites and making them into a single site, so that they can maintain it appropriately.

The defacement messages were classified into four groups and studied: (1) inoffensive, (2) slightly offensive, (3) offensive and threatening, and (4) extremely offensive and threatening. GForce has been leaving messages that are extremely offensive. Moron and Nightman have been hacking on a much larger scale, but their messages are slightly moderate compared with GForce. The messages posted by the WFD have been largely offensive. The Pakistan Hackers Club has not been placing significantly offensive messages. For example, the Silver Lords' messages about "Free Kashmir," using vile language and threats, exemplify offensive and threatening messages. GForce messages are also extremely offensive and threatening. They provide an example of Pakistan Hackers Club activity. Inoffensive messages contain content such as, "We defeated India."

An analysis was conducted to identify the trigger factors. Newsworthy events were divided into three groups. The first group was news of nuclear-related events. An attempt was made to see if the attacks on Indian sites were related to news of nuclear-related events. Thirty nuclear policy announcements were considered. They had no relevance to the attacks that took place. Statements or bomb explosions do not seem to affect the attack trends in any way.

Second, terrorist-related events were examined. The first one occurred on August 8, 2000, when Hizbul Mujahideen revoked the ceasefire declaration and its commandos went underground. On January 13, 2001, Jammu and Kashmir Chief Minister Dr. Farooq Abdullah escaped an attempt on his life. Researchers found that every one of these terrorist-related events was preceded by, or correlated with, excesses or increases in attacks on Web sites, all of which originated from the same groups. There is no doubt that these are related to each other.

Third, an effort was made to see whether government policies and responses to terrorist acts have decreased or increased the number of attacks. There does not appear to be any correlation.

The terrorist operations that have been taking place on land seem to have a very strong correlation to the number of cyberattacks, however small, that have occurred. There is also a very high correlation in the way that attacks have occurred. In monitoring attacks, there are asocial triggers that become clear, making it possible to predict the formation of attacker groups. It also becomes possible to identify triggers and to predict whether there is going to be a ground attack following a cyberattack. The third point is that preventive measures can be taken before cyberattacks are committed. There are several technologies available.

The Writing on the Wall

In India it is not hacking that has been on the rise, but rather *hactivism*. Hactivism is the convergence of political activism and computer attacks. Many hacker sites have been set up by nongovernmental organizations and antinuclear groups that use international funds and serve as front organizations. They have participated in chat groups, and psychological Web sites have been designed to create panic and to incite hate

groups. There are also Web sites that collect money through the Internet to fund antinational activities in other countries. Case studies show a direct relationship between political conflicts and increased cyberattacks. Malicious cyberactivity can have concrete political and economic consequences. Although more study is needed, in India cellular phone traffic appears to be a predictive indicator of the onset of terrorist acts. Cellular phone traffic should be closely monitored to detect anomalies that correspond to triggers. In India, as in Israel and Palestine, the number of cyberattacks increases following events such as car bombings and mortar shellings. Subsequent to the April 2001 midair collision between a U.S. surveillance plane and a Chinese fighter aircraft, Chinese hacker groups immediately organized a massive and sustained week-long campaign of cyberattacks against U.S. targets. There have been similar occurrences in India and constitute a type of political activism and are not for economic gain.

Often the intent of attacks is Web site defacement or denial of service. However, on several occasions, poor judgment on the part of patriot hackers has resulted in the hacking of the sites of organizations that are clearly not responsible for the attacks. In fact, one hactivist group erroneously defaced a site operated by a company with offices in the World Trade Center.

"Virus propagation" recycles or modifies old viruses to make them appear to be related to recent events. For example, a new version of the life_stages.txt.shs virus was renamed wtc.txt.vbs in order to give the appearance that it was related to the World Trade Center. New viruses and attacks sprang up with reference to the September 11, 2001, attacks. One example is the Goner virus, which appeared in December 2001.

As with the Comprehensive Test Ban Treaty, the ability of nations to launch cyberattacks and to protect against concerted attacks will become an item for negotiation among nations. As with the nuclear issue, there will soon be nations that are capable of protecting themselves from cyberattacks and non-cybernations. We are all vulnerable. It is important not just to rely on science and technology for protection. It is important to have sufficient analytical capability to learn from the traffic. With Internet Protocol Version 6 there is enough address space for every molecule in the world, and we should be able to assign that space such that the ownership is identifiable.

The future of intelligence is actually the open source. In fact, open-source information can be used to identify triggers. The challenge is to mine this information and find connections between apparently unconnected events. There is a theory that says that in the world every two persons are connected by six degrees of connectivity. The theory applies to terrorists and to persons who are trying to control terrorism. Open-source intelligence and networking strive to reduce this connectivity to two, so that it can be managed.

NEW DIRECTIONS IN THE MANAGEMENT OF CYBERTERRORISM

Every individual should have a traceable identity to guard against the creation of false identities. There must be a balance between privacy and national security. Every computer or access device is identifiable and traceable; every transaction is traceable.

The future of intelligence is in the open source. Through data mining to interlink apparently unconnected events combined with information fusion, recovery procedures,

and the use of cryptography, every computer or even every molecule could be given a traceable ownership.

RESEARCH ISSUES AND RECOMMENDATIONS

The following items indicate priority areas for further research.

- sensors for predictive analysis based on the flow at the backbone level
- information sharing
- data mining tools not only to predict attacks in advance, but also to predict low-intensity, long-duration attacks and the formation of groups
- data mining to interlink apparently unconnected events
- information fusion
- recovery procedures and CERT-In
- use of cryptography

The Lessons

In today's borderless world, protecting the world is everyone's business. Terrorism was once the problem of the developing nations. Today, it is everyone's problem. If we see terrorism in some other part of the world and keep quiet, we will live to regret it, because it will reach our doorstep very soon.

Under Indo-U.S. collaboration, it is necessary to share our experiences and expertise in information and communication security. To begin this process, experts from the two countries could develop a framework to be used by governments in protecting the cyberspace of each nation. This framework could involve regulatory mechanisms, technologies for developing monitoring sensors and analysis capability to predict intrusions well in advance. The second major area for collaboration is the creation of cybersecurity awareness across a wide spectrum of users, including homemakers, students, corporations, software and hardware developers, vendors, and government officials. Such awareness would greatly facilitate our efforts to protect the infrastructures of both nations.

5

Cyberterrorism and Security Measures

S.E. Goodman

It would be more productive to expand our scope from "cyber terrorism," a term lacking a widely accepted definition, to consider the following two pertinent questions:

1. What would terrorists want to do in cyberspace?
2. How do we try to deal with such activities?

To address these key questions, we first need to define our basic "who" and "what" we are discussing: Who are "terrorists"? What is "cyberspace"?

Terrorists are people, acting alone or as members of substate organizations (possibly with the support of a national government), who are deliberately trying to inflict mass casualties or cause other forms of costly consternation against civilian populations. At a minimum, these acts are intended to frighten these populations and to attract national or international attention.

Cyberspace is the set of all computer-communications networks. It is a major technology-enabled medium providing means of passage, the locus of objects of value, and parts of the control and management systems for critical processes and infrastructures.

The Internet is the largest single component of cyberspace, with a presence in more than 200 countries and approximately 1 billion users. For the most part, the Internet is built upon national and international telecommunications infrastructures, including the landlines of most public phone systems and wireless, and satellite communications. Beyond the Internet, these telecommunications infrastructures are more generally highly dependent on computing technology. Thus, by our definition, they are part of cyberspace.

Other critical infrastructures in the United States, and increasingly elsewhere in the world, depend on computer-communications systems for direct control and other functions. These include major forms of transportation, banking and finance, energy distribution, emergency preparedness and response, and public health.

Digital control and supervisory control and data acquisition systems (DC/SCADA) are computer-communications networks that are used by many

infrastructures and industries to manage sensitive processes and physical functions. DC/SCADA systems now more commonly use the Internet to transmit data and control instructions rather than the dedicated networks that had been used before. These should be of particular concern with respect to terrorism.

Very few of the "cyber" parts of these infrastructures were designed or implemented with security as much of a consideration, if it was considered at all. Most are riddled with vulnerabilities, which are defined as weaknesses that can be exploited through either hostile attack or accident. Many of these systems were designed to provide cheap and extensive network access. Unfortunately, this greatly increases the ability of malicious people to find and exploit vulnerabilities.

What do we know or anticipate that terrorists want to do in cyberspace? I believe the answers to this question fall into three categories:

1. to support their activities and infrastructure, but not directly through an attack
2. to explicitly attack parts of the cyber infrastructure
3. to use cyberspace as a means of attacking other targets

It is certain that terrorists and their supporters have been engaging in extensive activities under category 1, and that they will continue to do so.[22] This would cover communications, including encrypted communications with each other; recruiting and "advertising" (for example, via Web sites); and financial transactions such as money transfers and laundering. They are also likely to be scouring cyberspace for information on potential targets and on weapons of mass destruction.

Examples of attacks under category 2 might include massive distributed denial of service (DDOS) attacks to bring down parts of a national or international information infrastructure for the purpose of humiliating governments or other parties (for example, high-profile or symbolic multinationals and religious organizations), and precision strikes against the communications of selected targets during intense crisis periods. Note that cyberspace can be attacked physically–by cutting communications lines or blowing up switches or computers with critical databases–as well as cybernetically.

Possible attacks under category 3 would include compromising transportation or other supervisory control systems to cause disasters resulting in extensive consternation and costing many lives (for example, air traffic control, routing shipping containers, and process control for toxic chemical production). Cyber attacks might also be launched in conjunction with more traditional forms of terrorist attacks in order to severely exacerbate the consequences. For example, interference with the communications of emergency responders might occur during a biological attack.

There have been several malicious attacks, accidents, and experiments via the use of red teams or simulations that convince many people that very serious attacks under categories 2 and 3 are possible. These include both "broadcast" attacks like those now commonly associated with viruses, and more precise, focused, sustained, and sinister attacks. We have yet to see the latter in a truly devastating form.

[22] Weimann, Gabriel. 2006. *Terror on the Internet,* United States Institute of Peace Press, Washington, D.C.

It seems likely that there may be efforts by terrorists and others who serve them, to conduct probes or experiments along lines that might lead to attacks under categories 2 and 3.

As far as we can tell, terrorists have not been responsible for any of the major attacks or accidents that have occurred in recent years under categories 2 or 3. So much has been written about such possibilities–and they have had some prominence in the media–that it is inconceivable that terrorists are not aware of them. So far, for reasons we can only speculate about, they do not seem to have chosen to pursue these possibilities with vigor and effect, or perhaps they have tried and failed.

DEALING WITH CYBER-TERRORISTS

It would seem prudent to expect that such attacks will be launched sooner or later. Therefore we should ask ourselves the following: How do we try to deal with terrorists in cyberspace? We start to answer this question by distinguishing between two forms of defense: passive and active defense.[23]

Passive defense is essentially target hardening. It largely consists of the use of various technologies and products (for example, firewalls, cryptography, intrusion detection) and procedures (for example, those governing outside dial-in or reconstitution and recovery) to protect the information technology (IT) assets owned or operated by an individual or organization. Some forms of passive defense may be dynamic, such as stopping an attack in progress, but by definition, passive defense does not impose serious risk or penalty on the attacker.

Active defense by definition imposes serious risk or penalty on the attacker. Risk or penalty may include identification and exposure, investigation and prosecution, or preemptive or counter attacks.

With only passive measures, the attackers are free to continue the assault until they either succeed or get frustrated and look elsewhere. Given the vulnerabilities of most cybersystems, the low cost of most attacks, and the ability of attackers to strike from positions of physical safety, a skilled and determined attacker may be more likely to succeed than to become frustrated.

Some defensive actions, for example stopping an attack in progress, can be pursued using both passive and active means. Passively, the defender might plug a vulnerability hole in real time. Actively, the defender might try to locate and get back to the source of the attack.

For several legal and other reasons, most forms of active defense will necessarily fall to governments.[24] The effective pursuit of active forms of defense, with a high probability of correct identification and few false positives, is very challenging technologically.

---

[23] Goodman, Seymour E. 2003. "Toward a treaty-based international regime on cyber crime and terrorism," *Cyber Security: Turning National Solutions into International Cooperation*, Center for Strategic and International Studies Press, Washington, D.C., pp. 65-78. See: http://csis.org/pubs/2003_cyber.html

[24] Goodman, Seymour E., Stephen J. Lukasik, and David W. Longhurst. 2003. *Protecting Critical Infrastructures Against Cyber-Attack*, Adelphi Paper 359, International Institute for Strategic Studies, London, U.K. See: http://www3.oup.co.uk/adelph/hdb/Volume_359/Issue_01/

THREE STAGES OF DEFENSE

In discussing more explicit forms of dealing with terrorist activities in cyberspace, it will be useful to consider three stages of defense:

1. Prevention: How can we keep an attack from being launched? How can an attack be made to fail before reaching the target?
2. Incident management, mitigating an attack, damage limitation: An attack has reached the target. How do we prepare for and conduct defense during an attack? How do we defeat the attack without loss? How do we identify and limit damage?
3. Consequence management: What to do after an attack?

For each of these stages, I will illustrate several basic approaches. A much more detailed and comprehensive breakdown is given in *Protecting Critical Infrastructures Against Cyber-Attack*.[25] That source has a number of extensive tables organized by strategic objective (for example, mitigating cyber attacks). A set of strategic options appears under each strategic objective (for example, system owner terminal defense), and specific tactical objectives are listed under each of these (for example, defend against insiders). Required capabilities for each tactical objective (for example, compartmentalization on a need-to-know basis) and assessments of the locus of primary and secondary roles of responsibility (for example, primary role for owners and operators) follow.

Note that the implied sequential nature of these stages is really an ongoing feedback loop. Attacks and the risk of attacks are a long-term hazard in cyberspace. With each attack, whether successful or thwarted, both the attacker and defender learn lessons that presumably will help make them better at what they do.

Prevention

A basic approach is to design the system to be secure from an attack from the beginning. If this is done properly, attacks may be prevented because they would be perceived to be futile, or if launched, they would cause no damage. A coarse analogy is that people armed only with rifles rarely attack heavy tanks.

For the vast majority of IT systems, security was not a major design criterion, if it was considered at all, even with the original Advanced Research Projects Agency Network (ARPARNET), which was developed by the U.S. Department of Defense. If security were made a major design criterion for a new system, there is no doubt that it could be made more secure than most of its predecessors. However, there should be no delusion that we know how to design large, complex systems that can be kept and guaranteed safe and secure in today's world.

Since almost all cybersystems were not originally designed with security in mind, we have an enormous legacy of insecure systems that are used extensively. Improving security for such systems is largely a matter of afterthoughts and patchwork. The problem is compounded by security often being in conflict with design criteria that best promote

[25] Lukasik, et al.

the primary intents and needs of the organization. Access and throughput are examples of such design criteria. Added security is not just costly; it may also result in reduced efficiency and functionality.

Furthermore, so far there does not seem to be much incentive for people to design or redesign systems to be much more secure. There has been much speculation that the design or redesign of systems will occur only in the aftermath of a "digital Pearl Harbor" or in response to the forces of legal liability or insurance necessities and standards.

A postdesign and implementation variant is to try to prevent attacks by finding and fixing vulnerabilities before an attacker can try to exploit them. Red teams, test beds, or simulations may be used to do this. Another approach, at least to the often-serious threat of possible insider attacks, is to more thoroughly screen employees with potentially sensitive access.

Another general way to try to prevent attacks is to take measures to ban them. This is most obviously done through domestic laws that define such attacks as criminal acts. Given the transnational characteristics of many networks, there would also have to be precise, internationally recognized norms and technical standards. The basic precept is that most people are law abiding and will not engage in criminal acts that are explicitly forbidden, and which carry a heavy penalty.

Given the many technical and evidentiary problems of identifying cybercriminals and prosecuting them, nobody has any delusion that such laws would end criminal or terrorist activities in cyberspace. Nonetheless, they might reduce the enormous amount of malicious "noise" in cyberspace, and this would help make it easier to more readily identify more serious activities. They would also provide a necessary basis for encouraging people to report malicious cyberactivities, and for international cooperation in dealing with several kinds of problems.

Deterrence has made a name for itself in other contexts, most notably in strategies for avoiding nuclear exchanges during the cold war. We can conceive of analogies in cyberspace. These would consist of declaratory policies that would be backed up with technical capabilities that provide a high probability of detection, identification, and retaliation or other forms of risk. Deterrence is an implicit or explicit form of intimidation. We must presume that the party who practices deterrence is prepared to respond and is capable of acting effectively in response to a triggering event.

Various forms of preemption or interception may also be possible in this domain. Preemption is usually thought of as a counter-strike against an adversary who is about to attack. Interception is stopping an attack that has been launched from reaching the target. Both may be viewed as forms of prevention that are intensely urgent. Preemptive strikes or interceptions may be either cyber or physical. In cyberspace, the detection of intent and planning or of an early warning of an attack is especially intelligence intensive.[26] Those who poke around cyberspace looking for intelligence and indicators may run into all sorts of jurisdictional, privacy, and other legal constraints and problems. There is no effective cyber-equivalent of detecting the initial heat and light given off by a missile being launched.

Of the three main stages of defense, prevention has more active forms than the other two. The need to identify attackers or potential attackers, and to convince them that

[26] In the United States, many of these activities are undertaken by the National Infrastructure Protection Center.

there is a high probability that they will be punished is explicit or implicit in each of our discussions of prevention.

Most forms of active defense will have to be conducted by governments. Intergovernmental cooperation will likely be an impetus for the further development of active defense strategies in areas such as the exchange of intelligence. In many cases, private entities engaging in active defense run the risk of being identified and mistaken for criminals.

From a risk perspective, individual terrorists and terrorist organizations (even those supported by nation-states) are different from nation-states. Plausible denial is not important. Terrorists and terrorist organizations have few assets and no sovereign territory to protect from physical or other forms of counterattack or embargo. As a result, they are not sensitive to most of the possible consequences from nation-states that identification might entail. Terrorists who are prepared to perish during a spectacular attack may be less sensitive to preventative measures such as deterrence than criminals, industrial spies, hate mongers, or agents of nation-states who engage in other forms of cyberconflict.

On the other hand, given the possibilities of catastrophic terrorism, it is particularly important for the defense to try to prevent attacks and identify and apprehend or otherwise punish potential attackers.

Incident Management, Mitigating an Attack, Damage Limitation

The first order of business in this stage of defense is to provide indications and warnings that an attack is taking place. This is easier to do at this stage than it was in the prevention stage. Nevertheless, it is difficult, and intrusion detection has become a particularly active area in research and development. Not surprisingly, detection and notification are more difficult and prone to false positives during the early stages of an attack, before significant damage has been done.

To prevent penetration of the system at risk from the outside, we try to erect barriers and otherwise harden it. Both cyber and physical approaches are necessary. Passwords are the oldest, and still most widely used, cybertechnique. More recent and somewhat widely used techniques are firewalls and proxy servers. Like all forms of cyberdefense, these can be defeated, although it is possible to make them real barriers against many attempted attacks. Physical protection needs to consider several forms of penetration or attempts to isolate the system. These include attacks on electronics using electromagnetic pulses, and attempts to cut cable endings. A wide variety of forms of physical protection are possible, ranging from fences to biometrics.

If the system is penetrated from the outside, a next line of defense is internal compartmentalization and containment. In this instance, the goals are to limit penetration and damage, protect surviving assets, and protect and gather information to help with recovery and response after the attack. Approaches include creating internal physical barriers and cyberbarriers through compartmentalization and need-to-know access controls, intrusion tolerance schemes, setting up decoys, maintaining protected redundancies, and hiding assets. All have both static (pre-positioned and unchanging during the attack) and dynamic variants.

Another approach is automatic or partial shutdown and reallocation. A system that

senses it is under attack would start erecting internal barriers that would not be tolerable during normal operations, in an attempt to isolate those parts of the system that had been compromised. It would also involve load-shedding strategies to reallocate surviving capabilities to the most important functions required by the organization. All of this amounts to various forms of real-time reassignment and reconfiguration under rapid degradation.

Particular attention needs to be given to preserving and collecting information during an attack. This is done largely through audit and backup. Most defenders will need to find the most recent "clean" (pre-attack) state to facilitate effective recovery and resumption of operations. This is done most easily if the attack has a clear and precise starting time and backups are made regularly, or if the organization maintains a redundant "shadow" system. More insidious attacks that build up slowly and surreptitiously present a much more difficult problem in identifying a state where the information is uncorrupted and the system is free from inserted malicious code. It is also important to have strong audit functions to identify after the fact when an attack started and to collect information that might assist in the identification and apprehension of the attacker and help the organization better defend itself against similar attacks in the future.

Organizations should establish security policies and plans for defending against attacks. Comprehensive planning should cover a spectrum of possible attacks that pose particular risk to the organization. They should include assessments both of requirements for essential functions and of particular needs in all of the defense categories discussed previously. Special attention should be given to preventing and dealing with insider attacks. Staff should know who to call for help. It might be a good idea to test the plan through the use of exercises. However, most organizations avoid live "fire drills" because they can be expensive, disruptive, and risky in their own right. Many information systems are delicate and their owners are afraid something will go wrong, resulting in the self-inflicted equivalent of a serious attack.

Generally, we do not know how to design provably secure large, real-world systems. That goal may prove illusory, even from a theoretical standpoint. The various defensive approaches briefly described here are fairly general and should be pursued to protect both new and existing systems. None of them should be considered sufficient in and of itself. Taken together they form a multifaceted defense approach.

Increasing the security for DC/SCADA systems poses particularly difficult problems. These systems are often small and self-contained, and have constrained power needs (including backup). Security may not readily fit with the space, real-time, or power requirements. Security measures could also reduce performance or be problematic in the synchronization of other more extensive processes. Additionally, most of these systems are in the private or mixed sectors (for example, airports). Their owners and operators may not have sufficient resources to secure them more effectively.

From the standpoint of counter terrorism, we would imagine that attacking physical targets via control and management systems would result in the kind of mass casualties, damage, fear, and loss of confidence that terrorists favor. Many of these systems are vulnerable to tampering with control signals, especially by insiders. These category 3 uses of cyberspace by terrorists should be of particularly great concern.

Most of the activity at this defensive stage is passive and might be described as "terminal defense," because it is in the hands of the owners and operators of parts of

cyberspace who are mostly in the private sector. Serious questions remain as to who is responsible for defending the common areas in cyberspace, and how it would be done.

Consequence Management

There are two primary substages in this stage of defense: recovery and response. Recovery is largely about reconstituting IT assets so that the organization can operate as close to normal as possible as soon as possible. It is a passive form of defense. Response is concerned with identifying and punishing the culprits and learning lessons to enable the organization to better defend itself in the future. It is thus a more active form of defense.

A sample of the tasks that would fall under recovery might include

- the removal or shutdown of hostile or defective entities
- a damage assessment survey of what is broken or altered, and what is not
- an automated or semiautomated process for assessing and quickly and effectively rationing and reallocating what is left
- prioritization of functions to be reconstituted
- restoration to pre-accident or pre-attack status without destroying evidence

Carefully conceived and executed attacks can make recovery more difficult. For example, attacks that corrupt data or insert malicious code can be executed covertly over long periods of time and masked so that it will be difficult to know where to go for an unpolluted backup. Such corruption can take place over an extended time, simultaneously with the addition of many legitimate transactions that the owner does not want to lose during recovery. To date, most organizations that have suffered short-term attacks seem to have been able to recover fairly quickly and effectively, or at least they are not talking about their failures in this regard.

Tasks that would fall under response include

- getting the right culprit: strong forms of accurate trace-back and forensic tools, perhaps some kind of "fingerprinting"
- measured retaliation: legal principles of in-kind and proportionate retaliation
- asymmetries: what to do about attackers with few IT assets or vulnerabilities?
- escalation: rating the damage to decide if we want to send a very strong message

As was noted under the discussion of prevention, some of the singular features of high-impact terrorists make revenge more difficult, although it is probably more pressing than it is for ordinary cybercriminals, industrial spies, or agents of foreign governments. Terrorists are likely to be particularly dangerous people who intend to keep attacking. Presumably by this stage we know that we have been severely attacked by terrorists.

A brief assessment of our overall capabilities to deal with terrorists using cyberspace would conclude that for most potential targets, we are technologically and procedurally weak in every aspect the three stages of cyber defense against skilled, patient, and determined attackers who are not likely to be easily deterred.

Although there has been, and continues to be, much discussion of what needs to be done about research and development and funding, so far there has been a lack of significant advances or the extensive application of security technology that is already available.[27]

Vulnerabilities are found almost every time serious attackers or red teams look for them. Systems are so complex that fixing some vulnerabilities just forces attackers to find others (or the fix may even create new vulnerabilities). The number of successful attacks, many of which go unperceived by their victims, continues to grow at least as fast as cyberspace itself. In 2003, the number of broadcast attacks by worms, viruses, and spam was record setting. Even old technology such as passwords and firewalls are not used as extensively and effectively as possible, and are often compromised. All of this occurs in spite of a heightened awareness of security problems and needs.

Part of the problem is a combination of massive connectivity, with emphasis on widespread access, and a huge number of owners, operators, and users of cyberspace with greatly varying needs, motives, and resources. The domain of actors is much larger and more diversified than is the case with more traditional security issues.

Security is reasonably effective in only a few areas. These include cryptology and software for dealing with worms, viruses, and distributed denial of service attacks similar to those we have already encountered.

One area of concern that extends broadly across all of the stages of defense is the problem of insiders–people who have authorized access with the potential for abuse that can cause great harm. Insiders still probably account for a majority of successful penetrations for criminal purposes. The problem is complicated by changes in organizational relations and technical architectures that make "inside" and "outside" more difficult to even define. The possibility that a terrorist or a terrorist sympathizer might gain employment that would enable him or her to conduct a devastating attack or to provide critical information or access to others cannot be discounted or ignored. The two most general ways of dealing with infiltration are through deep pre-employment investigations, something that most non-government entities are neither capable of doing

---

[27] Computer Research Associates. November 16-19, 2003. *Four Grand Challenges in Trustworthy Computing*. Washington, D.C. See: *http://www.cra.org/Activities/grand.challenges/security/*; Defense Advanced Research Projects Agency. 2003. *Advanced Technology Office, Program Overview: Information Assurance.* Briefing for the National Security Telecommunications Advisory Committee, December 16, 2003. Several Defense Advanced Research Projects Agency offices have extensive research and development agendas related to cybersecurity. See: *http://www.darpa.mil/ato/programs.htm* and *http://www.ncs.gov/NSTAC/nstac.htm*; Institute for Information Infrastructure Protection. 2003. *Cyber Security Research and Development Agenda*. Hanover, NH. See: *http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf*; Lukasik, et al. cited above, and; National Research Council. 2002. *High Impact Terrorism, Proceedings of a Russian-American Workshop*. Washington, D.C. See: *http://www.nap.edu/books/0309082706/html/*. National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism,* National Academy Press, Washington, D.C. See: *http://www.nap.edu/html/stct/*. President's National Security Telecommunications Advisory Committee (NSTAC), the White House Office of Science and Technology Policy (OSTP), and the Georgia Tech Information Security Center (GTISC). May 13-14, 2003. *Research and Development Exchange Proceedings: Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness.* Georgia Institute of Technology, Atlanta, GA. See: *http://www.ncs.gov/nstac/r&d2003theme.html*

nor permitted to do in many countries, and through stronger forms of containment and compartmentalization of access within an organization.

Is cyberspace more secure today than 6 or 10 years ago? We do not even know how to provide a definitive answer. Most of us think the answer is no. For example, we believe that the growth of the Internet in the number and variety of connected new software and people, and the additional vulnerabilities this brings, is most likely outstripping the additional security being instituted by organizations and individuals.

Several countries have given visible attention to national plans or strategies to secure cyberspace.[28] The U.S. National Strategy to Secure Cyberspace is largely voluntary and suggestive. To date it does not seem to have resulted in dramatic improvements either within the U.S. government or in the mostly privately owned and operated national information infrastructure. If an effective Indian national cyberprotection strategy exists, I am not aware of it. Perhaps the development of a draft of such a strategy could be undertaken as a valuable joint project. The effort might also shed light on some possibilities for improving the U.S. national strategy.

The three technological areas that I believe need the most immediate attention to deal with potential high-impact terrorism are

1. technology for effectively gathering, evaluating, and acting on intelligence
2. more secure DC/SCADA systems for managing critical physical and telecommunications infrastructures
3. upgrading the capabilities and security of the information technologies for emergency responders

Those who pursue counterterrorism measures must bear in mind that terrorists can easily hide within the societies they intend to harm, avoiding exposure until they actually carry out an attack. This is true in both physical space and cyberspace. Consequently, counterterrorism in both physical space and cyberspace is necessarily intelligence intensive. Terrorists and fellow travelers engaging in activities in category 1–which includes many who are not explicitly interested in pursuing what might be called cyberterrorism under categories 2 and 3 – are exposing themselves in a cyberspace shared and accessed by defenders. Counterterrorism must learn to take advantage of this exposure, and to do so without overly compromising civil liberties or rights (for example, privacy) of everyone who is not a terrorist. Perhaps the efforts that have received the most visibility in this regard are those that have been directed against terrorist financing.

Initiatives under the first recommendation, such as the use of data-mining approaches or seeking to develop technologies to facilitate accurate trace-back and identification, have run into technical, policy, and legal problems. The recently shut down Total Information Awareness (TIA – later renamed Terrorist Information Awareness[29]) project under the U.S. Defense Advanced Research Projects Agency (DARPA) is perhaps the most notable case in point. Technically, it is very difficult to

[28] Lukasik, et al. and The White House. February 2003. *The National Strategy to Secure Cyberspace.* See: *http://www.whitehouse.gov/pcipb/.*

[29] This program was first established by the Department of Defense in February 2003 to research technologies that would aid in the tracking of personal information such as credit card information. In September 2003 the program was terminated.

trawl through the vast expanses of cyberspace to obtain actionable intelligence without a huge number of false positives, and without the risk of compromising the civil rights of law-abiding citizens.

The pursuit of the first recommendation is also plagued with problems of jurisdiction that are greatly compounded by the easy transnational access provided by many components of cyberspace, most notably the Internet. What may be perceived as serious in one country whose cyberinfrastructure may be used as part of a terrorist action may not even make the legal radar screen of others that are part of an attack that crosses multiple sovereign physical jurisdictions. Most countries have given little or no thought to explicitly making serious crimes of the activities described under categories 1, 2, and 3. Seeking widely adopted national laws criminalizing activities under at least categories 2 and 3 is an important objective. Having such laws on the books may also legitimatize the subject of serious cyberattacks in ways that help achieve progress under the second and third recommendations as well. In addition, enforcement and prosecution of these laws are also critical elements of the cybersecurity. One possible Indo-U.S. project might be to look into the status of such laws in both countries, and to propose either new laws or explicit improvements to existing law. Such an effort would require substantial interdisciplinary participation.

All of cyberspace comes to the ground somewhere. Although not necessarily impossible, identifying and tracing a terrorist to a physical location is not easy. The effort is fraught with technical and jurisdictional problems. Nonetheless, cases of high-impact terrorism may be so singular that the effort needs to be made.

The owners and operators of DC/SCADA systems are a small, but very important, subset of users of cyberspace in our context. Under the second recommendation, potential vulnerabilities in this area are of especially great concern and must be given priority by those national governments that are in positions to do so. This would include providing various forms of assistance and technology to the private owners and operators of digital control and management systems. Particular attention should be given to transportation systems because for decades they have been highly favored by terrorists both as targets and as the means of delivering an attack.

Emergency response is plagued by severe fragmentation of communications between multiple players at both national and local levels. Among other problems, this makes for information and command-and-control problems during intense high-impact crises when the resources of many jurisdictions need to be brought to bear effectively and on very short notice. There are also problems with building, maintaining, and effectively using use of databases with critical information. For example, information on biological or chemical substances in a database for emergency first responders might quickly and effectively be brought to bear at the locus of a catastrophic attack. From a technological standpoint, regarding to the third recommendation it is not difficult to upgrade the capabilities and security of the information technologies for emergency responders in the United States and elsewhere. The primary retardants to making progress are political and financial.

Cyberspace is plagued by a great deal of conflict and by other problems that are beyond the scope of this paper. It is probably the fastest growing domain for a wide assortment of malicious activities and crimes, including nuisance hacking, Web site vandalism, fraud and other financial crimes, and the use of the Internet to lure children to

meetings that result in their assault, kidnapping, or murder. There are many other hostile, natural, and accidental cyberhazards. For example, spam and pornography plague tens of millions of users on a continuous basis, and computer accidents have turned off the lights in large geographic regions. As with other domains, terrorism is one very serious but relatively low probability threat on a spectrum of other hazards. From a cost and societal perspective, particular attention might be given to defenses against cyberterrorism that can also contribute to defense against other cyberhazards, and vice versa. This view has been voiced about other risk domains, such as defending against bioterrorism and improving public health capabilities more generally to deal with natural and accidental epidemics. All three of the recommendations mentioned in this paper should help to address these wider needs.

6

Discussion of Information Technology and Communications Security

Rear Admiral (Retired) Raja Menon and Kumar Patel,
Discussion Moderators

Discussion moderators Raja Menon and Kumar Patel agreed that India will face new and graver challenges to its information technology (IT) and communications sector as it grows more sophisticated. They also seconded the observations of Seymour Goodman and N. Balakrishnan that it is important to distinguish between hackers and defacers who have a variety of motives.

Menon and Patel asked a series of questions, to which the presenters offered answers, with others joining in the discussion as noted.

The first question asked was, can a state retain its technological advantage over terrorists, and how does it convert its technological superiority to practical use?

Goodman answered by saying that the state–terrorist relationship was extremely asymmetrical. While the state, because of its capacity, has a huge technological advantage over terrorists, the problem is that the kinds of nonlinearities associated with what terrorists do in cyberspace give leverage to those with relatively little technical capability. It is going to be very difficult to overcome this because nonlinear leverage has always been thought of as one of the great advantages of the networks. It gives a small number of relatively weak people extensive access to a lot of information, each other, potential recruits and sympathizers, and prospective targets. There is also a negative aspect of tightening access against terrorists or other malicious users more generally because it would compromise access and privacy for many, many more "good" users.

POLICING AND JURISDICTION

Several participants raised the issue of policing the Internet, and also of jurisdiction when tracking down cyberterrorism and bringing attackers to justice. It was noted that in India, the IT act is not intrusive, but Internet service providers (ISPs) are

statutorily bound to provide adjacent space for intelligence agencies. Canada, the United Kingdom, and Germany were introduced laws that would restrict the freedom of the Internet. The question of the adequacy of technical methods to police the Internet was raised, and whether a certain level of compulsion can be introduced, since companies were most reluctant to move in this direction. It was also asked whether there are other models of cybersecurity, perhaps derived from industry practices or from the quality assurance model.[30]

How do India and the United States compare or differ in their vulnerability to cyberattack? Does India need a critical infrastructure assurance group or infrastructure protection agencies?

Balakrishnan's response was that the problems in India and the United States are completely different. If you walk into an airport in India it is not uncommon to find that the computers are down and that they have switched to manual procedures. India now has an unreliable network, although it is not that poorly designed. Because of a variety of other infrastructure issues, sometimes the machines become unreliable.

He added that India's international gateway bandwidth is much smaller compared to its national backbone bandwidth, whereas in the United States, both are comparable. A campus such as Carnegie-Mellon University (CMU) has an Internet connectivity of about 3.5 gigabytes (GBytes), and the U.S. backbone is of the same order. In other words, CMU is the Internet. In India the Internet is completely different from the Indian network, and only a thin pipe connects the two, so it is not possible to take over the bigger network—India's system has an advantage as well as a disadvantage.

Is there a cause-and-effect relationship between cyberattacks and world events?

Balakrishnan's response was that cause and effect were actually like transformers; one is a transformer of the other, and very often, unless we also do a deeper study of the violation of the causality principle, it is very difficult to say which came first. However, he continued, what we know is that within a window of 1 week to 10 days, both of them peak. We cannot say that if cyberactivity increases, tomorrow morning there will be a terrorist attack, but a week's time is a more reasonable prediction that activity will flow up in both of them. This has been seen in several serious analyses of maps, methods, and so on.

As for the absence of suicide bombers in cyberspace, Balakrishnan noted that the problem is not only are there no suicide bombers, attackers' identities are also unknown, giving them a phenomenal advantage. In this respect, it is instructive to compare Indian and U.S. law. Whenever you talk about damage, you talk about two things: time and jurisdiction. In India the jurisdiction is related to the place where the damage has occurred; thus, if a house is bombed, the case will go to a local court, whereas in the United States, if there is any damage to U.S. property, it will be tried in a federal court. Balakrishnan noted that under Indian law, if he hacked a Pakistani site, he would go to jail, but if a Pakistani hacked an Indian site, nothing would happen because he is not covered by Indian law, which is incompatible with the question of jurisdiction and borderless crime.

Lewis Branscomb noted that the jurisdiction problem was very difficult, but that

[30] This model audits the quality control of companies to enable them to participate in government work; they have to meet certain government or military specifications.

for terrorism it really mattered because we want to capture the terrorist. A terrorist is not a cybervandal or a fraudster from a remote country, but it is physically difficult to apprehend somebody not in your own country. Branscomb noted a precedent in civil aviation hijacking, when the world decides not to tolerate a particular act and defines it as a crime. In civil aviation it is called interfering with airport and aircraft operations, and the political judgment is taken out of the hijacking issue. Airplane hijacking was a terrible problem in the 1970s, a hijacking every week or so, sometimes more than that. This became such a threat to civil aviation and to states' economies that almost 174 nations agreed to a sequence of treaties that universally declared hijacking a crime. There is something similar with extradition for murder; everyone recognizes murder as a common crime, and there are extradition agreements that bring people to justice.

Branscomb asked whether we could define a core subset of acts against cyberinfrastructure that the great majority of states would agree are crimes, and agree to cooperate in prosecution and punishment. The situation is complicated because not only can somebody from Pakistan attack somebody in India, but someone in Pakistan can go through 28 different countries and attack people in both India and the United States. No country is capable of physically locating and apprehending that person on its own. Branscomb stated that this was an example where near-universal international cooperation is absolutely necessary and feasible.

What about attacks on bandwidth?

Goodman answered that there were basically two ways to attack bandwidth. One is to clog it up, and the other is to remove parts of it. There were instances where there were such successful attacks that hundreds of millions of dollars in losses were attributed to them. Goodman noted that these were for short periods of time, and most of the losses were not lost transactions but delayed transactions; however, some technically knowledgeable people believe that serious, extended, sustained follow-up attacks are possible, and that this would seriously cripple bandwidth for extended periods of time, but so far this has not happened.

What about attacks for financial gain or to gain access to government intelligent networks?

Balakrishnan suggested that the billions of dollars lost worldwide to hacking can be classified into two categories: denial of a potential gain and actual theft of money. Together these constitute financial loss. In India, neither of them is possible. There is little e-commerce, with few Web transactions; if they fail there is still a parallel mechanism, simply using a phone. But in the United States, where many of the e-commerce Web sites are located, jamming these sites for about 2 hours leads to a loss of business, as the customer moves on to some other site. However, Indian insurance laws are very lax compared to U.S. laws, so if somebody steals from a credit card, there is still a loss to the holder of the card.

As for access to government intelligence networks, Goodman stated that he did not really know; government intelligence communities are even less likely than banks to report when they have been attacked. However, many intelligence systems have safety gaps, and are not connected to the kinds of networks that terrorists can access; terrorists might be able to access things that are considered to be of relatively limited value in loss if they are compromised. Terrorists are certainly looking around, trying to learn how to build weapons of mass destruction, and they seem to be collecting information (floor

plans for buildings and so forth) on how to attack various kinds of infrastructures. In the end, most intelligence agencies are compromised in the worst way by insiders, and Goodman said that he suspected that there were such activities going on also in South Asia.

Questions were posed about the acceptable cost of cybersecurity, that is, what is minimally acceptable, and how to measure cost not only in dollars and rupees, but also in inconvenience to system or Internet users. In response, Goodman observed that states could force the private sector to do better, but that it was a complicated issue. The United States has tried to put together national cybersecurity strategies, but was criticized because it did not put much pressure on the private sector, most of the actual owners and operators, to improve their cybersecurity. There is also the criticism that there has been little substantive public input despite the extensive use of various security products by individual private users, and these two criticisms may be related to that lack of input. Goodman noted that one real problem is the very diversity of the private sector; it has very different cyberspace needs and capabilities, and it is not evident what the government could insist that either the entire private sector or some subclass of it could actually do. Further, the government itself was reluctant to make demands on the private sector when it did not know exactly what to demand. This is what happened with Y2K, although one of the steps the government took that was cheap and apparently effective was to have the Securities and Exchange Commission insist that companies that were listed with them basically report to their stockholders on what they were doing to mitigate the Y2K threat.

Regarding quality assurance models, Goodman's judgment was that not only quality assurance but also such things as insurance have both distributed risk and raised standards in sectors such as home, auto, and fire insurance, but no one has been able to think of good models for cyberrisk. In that context, what little you see of cyberinsurance in the United States tends to be in the form of insurance with very limited coverage and very high premiums because the insurance companies do not know what to do, in the absence of good data; they are experimenting, but experimenting on the side where any errors are likely to favor them.

In replying to the specific question of what is an acceptable cost for cybersecurity, Goodman stated that nobody really knows, in part because cost issues are very complicated. Cost is not just a matter of dollars or buying more software, it includes people's time. There are now so many kinds of low-level attacks taking place that lots of staffs in computer centers typically spend about one-quarter of their time trying to deal with it, even in relatively low interest targets such as universities.

Goodman continued, adding security also is a functional problem. What does adding security mean? Does it mean looking at your customers more closely, limiting their access? That is a cost. Does it mean vetting your own employees to reduce prospective insider problems? That is a cost. Doing a lot of checking in real time or near-real-time reduces speed. Adding more security functions might squeeze or retard the kinds of functions that your organization really wants out of its cybersecurity. The bottom line seems to be that, for now, most organizations are taking the risk of attack. They are doing more, but perhaps not as much as keeping up with the risk and the threats, or eliminating the vulnerabilities that they might be able to eliminate.

Goodman also noted that in matters of cost and security, the U.S. government was

no paragon of virtue; many parts of it have been found desperately wanting. The reasons such agencies as the Departments of Energy, Homeland Security, and Defense, and others, have not been able to do much are cost and lack of expertise. Even if you want to do something, do you have somebody who can do it?

Goodman and Branscomb also elaborated on the "Orange Book," promulgated by the National Security Agency, which was supposed to deal with software acceptability and security. Goodman noted that it never became a popular resource, possibly because it was written before networking pervaded the industry. Branscomb elaborated on this, noting that the Orange Book was intended to establish levels of provable or demonstrable security in large operating systems in big computers. IBM never managed to make a computer that would qualify at the highest level, and in any case, did not have the incentive to do it even though the government would have wanted to purchase such a computer. In those days IBM's biggest customers were large financial institutions, insurance companies, banks, and the like, and the banks were so accustomed to accepting 2 or 3 percent defalcations (or embezzlements) as the cost of doing business and had therefore concluded that it was cheaper to absorb those losses than it was to spend that extra money to ensure every teller was honest. They treated computer fraud the same way. There is thus no market for secure systems for commercial applications; companies can absorb small losses. Branscomb concluded by noting that the reason there are very little government research funds for academics to study how to build secure operating systems is that the number of universities that formally train people in this field is very small and in general they are not considered excellent. This, he said, was a serious problem, and reflects the fact that our intellectual investments are influenced by a market economy.

LOOKING AHEAD

Regarding U.S.-Indian cooperation, Menon summarized some of the ongoing cooperative mechanisms between the two countries. These included the U.S. Department of State's Bureau of Political and Military Affairs, White House Office of Cyber Security, National Communication System, Department of Defense, White House Office of Science and Technology, National Infrastructure Protection Center, Critical Infrastructure Assurance Office of the Department of Justice, Carnegie-Mellon University, Defense Advanced Research Projects Agency, and Idaho State University. In India there is the National Security Council staff, which is the coordinating agency, the Intelligence Bureau, Navy, Army, Air Force, Ministry of Defense, Central Bureau of Intelligence, Department of Transportation, the Center for Artificial Intelligence and Robotics, and the Department of Information Technology. These entities have formed four task forces: (1) legal cooperation and law enforcement (under the joint chair of the National Infrastructure Protection Center and the Indian Intelligence Bureau); (2) information security standards and research and development (under the joint chair of White House Office of Science and Technology and Department of Information Technology); (3) information infrastructure protection (chaired by the National Informatics Center and the National Communications Center); and (4) defense cooperation between the Indian Army and the C3I Directorate of the U.S. Department of

Defense. Menon observed that this cooperation was less formidable than it sounded because the United States was years ahead of India in many fields; further, while many of the U.S. organizations are statutorily tasked with certain responsibilities against terrorism, including cyberterrorism and infrastructure protection, this is not so in India, which has some way to go.

This point was reiterated by Roddam Narasimha when he noted that the United States and India have different IT and communications infrastructure vulnerabilities, because they are at different stages of using networks. The Indian system is still less network dependent, so parallel mechanical systems are still operational. Yet there is widespread agreement that in both countries the vulnerabilities are very great and cybersecurity is still weak. This is one area where in order to ensure greater security, international cooperation is essential, although the mechanisms for doing this are not yet strong.

7

Threats to Civil Nuclear-energy Facilities

John P. Holdren

The possibility that civil nuclear-energy facilities might become targets for terrorists has been recognized since long before the attacks of September 11, 2001, on the World Trade Center and the Pentagon.[31] The principal attraction of civil nuclear-energy facilities[32] as terrorist targets lies in the potential for creating a release of radioactivity large enough to produce significant casualties and land contamination. Destruction of an important piece of energy-supply infrastructure in the targeted country and the possibility that a successful attack would lead to the wholesale shutdown of nuclear-energy facilities around the world might be seen as collateral "benefits" by terrorists.

Obstacles are in place to prevent successful attacks on civil nuclear-energy facilities. First, multiple security barriers would need to be breached in order to generate a large release of radioactivity. Second, guard forces and other entry barriers complicate the task of terrorists seeking to penetrate a facility in order to try to blow it up or otherwise create a containment-breaching event from within. In addition, the "hard target" characteristics of most nuclear-energy facilities make them challenging to destroy from the outside with the types of weapons terrorists are most likely to have at their disposal, namely rocket launchers, mortars, light aircraft packed with explosives, and hijacked airliners used as cruise missiles.

This presentation begins by locating the threat of attack on civil nuclear-energy facilities in the larger terrain of nuclear-terrorism dangers. It goes on to describe the potentially dire consequences of a successful attack, to discuss the range of scenarios through which such attacks could unfold, and to characterize in some detail the opportunities, barriers, and determinants of consequences that shape the risk associated

[31] See: Holdren, John P. 1974. "Hazards of the Nuclear Fuel Cycle," *Bulletin of the Atomic Scientist*, October, pp. 14-23; Ramberg, Bennett. 1980. *Destruction of Nuclear Energy Facilities in War,* Lexington Books; Hirsch, Daniel, Stephanie Murphy, and Bennett Ramberg. 1986. "Protecting Reactors from Terrorists," *Bulletin of the Atomic Scientists,* August/September.

[32] Civilian nuclear-energy facilities are considered nuclear-power reactors and their spent-fuel storage pools and nuclear-fuel-reprocessing plants, but may also include mixed-oxide fuel-fabrication plants and radioactive-waste repositories.

with this set of possibilities. It then draws on recent relevant experience and analyses to address what is being done to limit risk and what else could be done. The paper closes with the case for increasing international cooperation (and increasing Indo-U.S. cooperation in particular) in order to reduce the chance of a successful terrorist attack on a nuclear-energy facility in any country.

THE LARGER NUCLEAR-TERRORISM TERRAIN

Nuclear-terrorism dangers can be divided into three categories: (1) dirty bombs, meaning conventional explosives or incendiary devices that disperse radioactive materials, (2) attacks on nuclear-weapon or nuclear-energy facilities, and (3) terrorist acquisition and use of nuclear-explosive weapons.[33] Further, the mere assertion of the capability to carry out one of these kinds of attacks—or an explicit threat to do so at a particular time and place—may serve terrorist purposes, even if an attack does not occur. The public's deeply ingrained fear of nuclear weapons and nuclear radiation tends to amplify not only the impact if an attack is carried out, but also the terror effect of threats to do so.

Of these three categories of nuclear-terrorism dangers, the first one—the dirty bomb—is the easiest for terrorists to execute. In most circumstances, however, a dirty bomb would cause relatively few immediate fatalities beyond those caused directly by the chemical high-explosive used. (A conceivable exception could be the use of an incendiary device to disperse a potent radionuclide into the ventilation system of an office building.) The largest impacts of most dirty bomb events would be in property damage—the costs of temporarily abandoning and cleaning up the contaminated areas—and in the fear and demoralization created in the public.

Success in the second category of danger—attacks on nuclear-weapon or nuclear-energy facilities—would be far harder for terrorists to achieve, but could create considerably higher casualties. The impact of such an attack could involve hundreds or even thousands of immediate fatalities, tens of thousands of delayed deaths from radiation-induced cancers, and immense economic damage from the contamination of territory.[34] Success in the third category—that of acquiring and detonating a nuclear weapon—is likely to be the most difficult for a terrorist group to achieve. Nonetheless, such an attack could produce hundreds of thousands of immediate deaths (from the effects of blast and burns of a detonation in the heart of a major city), as well as numerous additional casualties from fallout and immense property damage.

---

[33] Nuclear-explosive weapons are those where most of the energy release comes from nuclear reactions rather than from chemical high-explosives.

[34] It has been well known since the 1957, U.S. Atomic Energy Commission study entitled "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants" (also known as "The Brookhaven Report"), that a large accident at a nuclear power reactor could produce thousands of prompt fatalities and delayed cancer fatalities in the many tens of thousands to more than 100,000. Subsequent studies have added many refinements but have not changed the upper-end figures. Subsequently, studies of large accidental releases from spent-fuel pools have generated similar results. If accidents at nuclear-power facilities could generate damages of these magnitudes, so could an 'accident' deliberately engineered by terrorists.

Since the September 11, 2001, attacks, there has been an upsurge of interest in terrorist potentialities. The attention of policy makers and of the public has been focused primarily on the first and third dangers, dirty bombs and nuclear explosives, but dangers in the second category should not be neglected. It is important to remember that risk—the probability of an event multiplied by the amount of damage that ensues if the event occurs—is often greatest for events of intermediate probability and intermediate consequences. Attacks on nuclear facilities fall into this middle range. They are more likely to succeed than attempts to acquire and explode a nuclear bomb, and at the same time, more damaging than a dirty bomb.

The rest of this paper focuses on this second category of dangers, and most particularly, on attacks on civil nuclear-energy facilities. However, many of the conclusions drawn herein would also apply to military nuclear facilities such as large plutonium-production reactors and the associated spent-fuel-storage and fuel-reprocessing facilities.

ASSESSING THE RISK

The probability side of the risk from attacks on nuclear facilities is influenced by the motivation of terrorists to pursue this route as well as by their capabilities in relation to the challenges of the task. The motivation presumably resides above all in that an attack on nuclear facilities has the very considerable potential for doing damage. A successful attack on a nuclear power reactor, for example, could destroy the facility itself, worth hundreds of millions to billions of dollars; produce tens to hundreds or even thousands of early fatalities and tens of thousands of delayed cancer deaths; and severely contaminate hundreds to thousands of square miles of land, requiring removal of much of it from habitation, commerce, and agriculture for periods ranging from months to many decades.

Such an attack would also cause terror and distress among far more than just the people physically harmed (amplified by the public's particular fear of radiation), deprive the affected region of an important component of its electricity supply, and probably lead to prolonged or even permanent shutdown of other nuclear power plants around the world, with serious economic consequences.

Beyond the question of the terrorist's motivation, risk depends on the actual possibilities for attacking nuclear-energy facilities—that is, the particular mechanisms and scenarios by which attacks could be carried out and the extent to which these are within the reach of terrorists to implement—and on the consequences that would ensue if these possibilities were realized.

Starting with mechanisms and scenarios, the possibilities fall into three main categories. First, as the September 11, 2001, attacks (and many novels) have underlined, terrorists could crash an airliner or a light plane packed with high explosives into one of a number of potential targets. A nuclear reactor or a reactor's spent-fuel storage pool rate among the most dangerous targets, but a mixed-oxide fuel-fabrication plant (made an attractive target by the presence of plutonium), a dry-cask spent-fuel storage facility, a spent-fuel shipping cask in transit, or a nuclear-waste repository are other possibilities. Second, terrorists could attack a facility or item in transit with mortars or rockets or

emplaced explosives. Third, they could mount an attack using an armed force, possibly aided by insider accomplices, to gain entry to a facility in order to use explosives or other means to try to release radioactivity.

How many of the most dangerous targets are there? In the United States there are 103 operating power reactors at 65 sites. India has 14 power reactors at 6 sites, and 8 more reactors under construction. Worldwide there are 440 power reactors and 32 more under construction.[35] Each reactor site has a spent-fuel storage pool containing typically several times as much long-lived radioactivity as a reactor. In addition, large civil fuel-reprocessing plants are in operation at La Hague (France), Sellafield (England), and Chelyabinsk region (Russia); similar but smaller commercial plants operate at Tokai-Mura (Japan) and Marcoule (France).

How vulnerable are these targets? Reassuring statements from nuclear-industry groups and advocates are easy to find.[36] However, the more balanced National Academy of Sciences study, *Making the Nation Safer*,[37] and a range of other papers by unbiased analysts suggest that the picture is mixed. The prevalent view is that it would not be easy to attack a nuclear-energy facility in a manner that succeeds in releasing a large quantity of radioactivity. At the same time, experts agree that such an attack is not impossible and may not even be unlikely over the course of time unless additional protective measures are taken that can offset the likely increases in the capabilities of terrorists.[38]

What is the possibility of an attack on a nuclear reactor? Containment buildings at a few U.S. reactors located near airports were explicitly designed to survive the impact of a 707-class airliner moving at around 200 knots (representing speeds on approach to landing or shortly after take-off). The design-basis threat for containment buildings at all other nuclear reactors was not an external impact but an internal steam explosion. Despite this fact, the U.S. Nuclear Regulatory Commission (NRC), in retrospective analyses, determined that most containment buildings would be able to survive the impact of a 727-class jetliner traveling at 500 knots. It is less likely that U.S. reactor containments would survive the impact of a 767-class airliner traveling at 500 knots. Further, it is noteworthy that some reactor containments outside of the United States are less robust than those inside the country. The impact of a light aircraft packed with high explosives could be problematic for many containments both in the United States and abroad.

Reactors are generally protected by extra shielding inside the containment, but it is difficult to determine whether this extra protection would prove sufficient against the kinds of attacks from the air that are now plausible. Safety-related systems outside of the main containment could also lead to significant releases if they are destroyed at the same time that the containment is damaged by an attack from the air. Sabotage by intruders armed with high explosives is another scenario. If the intruders were to possess detailed

---

[35] International Atomic Energy Agency databases on civil nuclear-energy facilities. See: *http://www.iaea.org/DataCenter/*

[36] See, e.g., Chapin, D. et al. 2002. "Nuclear power plants and their fuel as terrorist targets" *Science,* Vol. 297, September 20, pp. 1997-98.

[37] National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, D.C. The report is available in PDF format at *http://books.nap.edu/hml/stct/index.html*.

[38] See also: Bunn, Matthew and George Bunn. 2002. "Strengthening nuclear security against post-September 11 threats of theft and sabotage," *Journal of Nuclear Materials Management,* Spring.

knowledge of reactor systems, they could likely produce a core melt event and steam explosions capable of breaching the containment, even without benefit of an aircraft impact or light-plane-as-cruise-missile attack from the outside.[39]

Spent-fuel pools may be more vulnerable than the reactors with which they are associated. The spent fuel in such pools can catch fire if the water is removed. Such fires can be difficult to extinguish and could release large quantities of cesium-137 and other radionuclides. An analysis published in 2003 found that spent-fuel pools in the United States currently hold an average of 400 tons of spent fuel each, containing 35 megacuries (MCi) of cesium-137.[40] A 1997 Brookhaven National Laboratory study concluded that a fire at such a spent-fuel pool could release between 10 and 100 percent of the cesium-137 inventory.[41] Hence, in an average case, between 3.5 and 35 MCi would be released. This amount can be compared to the approximately 2 MCi of cesium-137 that was released in the Chernobyl accident.

Fuel-reprocessing plants contain many reactors' worth of radioactivity but little stored energy. For these plants, large-aircraft impact is probably a bigger risk than sabotage from within. Dry-cask spent-fuel storage, spent-fuel shipping containers, and geologic radioactive-waste repositories are far less vulnerable than are reactors and fuel-reprocessing plants. Large radioactivity releases from attacks on these targets are very unlikely.

Of course, the consequences of a successful terrorist attack on any nuclear-energy facility depend not only on the quantity and kinds of radioactivity released, but also on wind direction, atmospheric-mixing conditions (which govern both vertical and horizontal spreading of the radioactive plume), the distribution of population in relation to the path of the plume, and the extent to which those in the plume's path can be evacuated before it reaches them. Unlike accidents, which occur at random, terrorists carefully choose the site of their attacks. Further, they might even succeed in choosing weather conditions that would maximize the impacts of an attack.[42] The 1997 Brookhaven study estimated the consequences of a spent-fuel pool fire at a pressurized water reactor to be 54,000 to 143,000 extra cancer deaths; 2,000 to 7,000 square kilometers of agricultural land condemned; and economic costs of $117 to $556 billion from evacuation.

---

[39] Most of the relevant official analyses of these possibilities are classified. While this is understandable—no one would favor publishing a handbook telling terrorists how to achieve their desired result—it is problematic because managers of U.S. civil reactor sites—and, I suspect, of other civil reactor sites around the world—historically have not had the security clearances needed to access this information. This is now being rapidly, if belatedly, addressed in the United States. I am not aware of the extent to which it is being addressed elsewhere or of the extent to which it will become possible to share some of these classified analyses across national boundaries. Clearly, if the officials responsible for managing reactor security are themselves unaware of the details of scenarios that could compromise that security, they cannot judge whether the protective measures being implemented are adequate.

[40] Alvarez, R. et al. 2003. "Reducing the hazards from stored spent power-reactor fuel in the United States," *Science and Global Security*, Vol. 11, pp. 1-51.

[41] Travis, R. J., R. E. Davis, E. J. Grove, and M.A. Azarm. 1997. *A Safety and Regulatory Assessment of Generic BWR and PWR Permanently Shutdown Nuclear Power Plants.* Report BNL-NUREG-52498. Brookhaven National Laboratory.

[42] Many people simply take reactor accident safety analyses and apply them to the problem of terrorism without noticing that the results generally presented for reactor accident analyses are averages over a wide number of sites and weather conditions. In addition, an attack involving the worst site or the worst weather can cause 50 to 100 times more damage than the average over all sites and all weather conditions.

SIGNS OF COMPLACENCY AND VULNERABILITY

We would expect that potential consequences of this magnitude would have led to a high degree of vigilance by those responsible for security at nuclear-energy facilities and a correspondingly high degree of confidence that attacks designed to create such consequences could be thwarted. Unfortunately, where we would hope to find a basis for confidence, there is instead considerable evidence of complacency and vulnerability.

Before September 11, 2001, once every 8 years each civil nuclear reactor site in the United States carried out a force-on-force exercise to simulate an attack by intruders. The site managers were advised in advance of the date of the simulated attack and were allowed, if they chose, to upgrade the guard forces to cope with it. According to a 2003 General Accounting Office (GAO) study, the upgraded guard forces were defeated in more than 20 percent of the simulated attacks. When the guard forces in place were at normal levels, they were defeated in more than half of the simulated attacks.[43]

Excessive "non-cited violations" by the NRC constitute a second sign of complacency and vulnerability. Non-cited violations entail no penalty and no follow-up. Most of the security shortcomings that are identified in routine NRC inspections are classified as non-cited violations on the grounds "that the problems had no direct immediate adverse consequences at the time they were discovered." This appears to mean that no terrorists were attacking the plant while it was being inspected. This may seem to be a harsh judgment, but the 2003 GAO study reported that in 2000 and 2001, the NRC issued no cited violations and 72 non-cited ones. The non-cited violations included the following instances documented by NRC inspectors.

- A security guard slept on duty for more than half an hour. The incident was treated as a non-cited violation because no attack had occurred during this period and because neither he nor any other guard at the plant had been found sleeping more than twice during the previous year.

- A security officer falsified logs to show that he had checked vital area doors and locks when he was actually in another part of the plant. In this case the officer was solely responsible for the security of the particular area because a security upgrade project was under way that had disabled or diverted all the other security for the area.

- Guards failed to physically search individuals for metal objects after the walk-through detectors and hand scanners indicated that something was present. These individuals were then allowed unescorted access through the plant's protected area. This was treated as a non-cited violation because a similar breach had been observed fewer than two times at that plant in the preceding year.

Moreover, the NRC does not systematically collect, analyze, and disseminate

[43] General Accounting Office. 2003. *Nuclear Regulatory Commission Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened.* GAO-03-752. Washington D.C.

information relevant to improving plant security. The 2003 GAO report on the security of U.S. nuclear-reactor sites found that the NRC does not have a routine, centralized process for collecting, analyzing, and disseminating security inspections to identify problems that may be common to other plants or to identify lessons learned in resolving a security problem that may be helpful to plants in other regions. NRC headquarters receives inspection reports only when a licensee challenges the findings from security inspections. NRC headquarter officials do not routinely obtain copies of all security inspection reports because headquarters files and computer databases are insufficient to hold all inspection reports.[44]

The NRC issued an extensive rebuttal to the GAO report, but it did not dispute these findings.

Another sign of complacency and vulnerability is that, in the United States, state laws often constrain the types of weapons that can be used by guard forces, virtually ensuring that they will be less well armed than their attackers. Specifically, state law often forbids the use of automatic weapons by nonfederal guard forces at nuclear power plants. Since attackers will probably be armed with automatic weapons, this asymmetry in weaponry hurts the prospects for the successful defense of nuclear power plants.

The existing laws of several states call into question the legality of the use of deadly force to protect private property. Many of the guards at these installations have expressed concern in interviews that were they to use deadly force against intruders, they might be subjected to legal action or punishment. The NRC has recommended that state legislatures and the U.S. Congress pass legislation to remedy this situation, but this has not yet occurred.

Many prominent members of the nuclear energy profession appear to be underestimating the terrorism problem, especially in statements prepared for policy makers and the general public. Claims such as, "nuclear power plants are the best protected industrial facilities in the United States" and "attacks on nuclear reactors cannot cause significant harm to the public" are common. The first claim is misleading because, although it might be accurate, it says nothing about whether or not the degree of protection is adequate relative to the threat. The second claim is wrong: the harm that could result from successful attacks on nuclear reactors has been established by many independent studies. Nor is the threat purely hypothetical: actual threats against, or attacks upon, nuclear power reactors have already been reported in Argentina, Lithuania, Russia, South Africa, South Korea, and western Europe. These events are listed in the database on nuclear terrorism that is maintained at the Monterrey Institute of International Studies and the Center for International Security and Cooperation at Stanford University.

RISK REDUCTION

How can the risks be reduced? Consider first some steps that have already been taken or are being taken in the United States:

- strengthening barriers to hijacking commercial aircraft

[44] Ibid.

- improving surveillance of general aviation (that is, light aircraft)
- revising the design-basis threats for armed and insider attacks and correspondingly increasing the capabilities at reactor sites to defend against such attacks
- holding force-on-force exercises at every nuclear facility in the United States every 3 years with the security forces that are specified in each facility's respective site plan
- tightening background checks and access control for temporary workers and visitors
- increasing the standoff distances maintained to preclude truck-bomb attacks
- reviewing and strengthening redundant reactor safety systems in light of upgraded aircraft impact and armed attack scenarios

What more could be done? Here are some additional steps that ought to be considered:

- ensure the appropriate dissemination of information between sites and headquarters, and among sites
- expand the no-fly zones around high-risk facilities
- provide additional physical barriers or active defenses to make it more difficult to fly an aircraft into a nuclear reactor or a spent fuel storage pool with the trajectory and the velocity required for a successful attack
- build additional dry-cask spent-fuel storage capacity to reduce pool inventories
- strengthen containment buildings
- place future reactors, spent-fuel storage, and reprocessing plants underground
- nationalize the guard forces at nuclear facilities in order to achieve standardized profiling and training, and upgraded weaponry
- improve evacuation, medical assessment, treatment, and decontamination capabilities

THE CASE FOR INTERNATIONAL COOPERATION

A successful terrorist attack on a nuclear facility anywhere would have consequences everywhere. This is true because large releases of radioactivity circle the globe. They create radiation doses over a wide swath and terror over an even wider one. A nuclear disaster anywhere would generate pressure to shut down civil nuclear energy everywhere. Such a shutdown could potentially have a severe impact on electricity supply, on the capacity to meet basic energy needs, and on the global economy. Thus, we all need to be interested in the security of nuclear facilities in all countries, not just in our own country.

Further, international cooperation to reduce the vulnerability of civil nuclear energy facilities to terrorist attack can

- facilitate learning from diverse experiences—including negative ones—and expertise available in different countries
- reduce the cost and increase the pace of security improvements because expertise and technology are being shared
- eliminate easy targets (which terrorists are able to seek out) by propagating best practices and raising the standard everywhere

Clearly, international cooperation ought to be encouraged in general, but it is particularly crucial between the United States and India. Laying the foundation for this relationship is one of the reasons the workshop in Goa was so important and so promising.

8

Threats to Nuclear Facilities: Framing the Problem

P. Rama Rao

This workshop does not solely address issues related to securing civilian nuclear facilities. It has a much wider scope encompassing several important issues pertaining to terrorism in general and its impact on specific domains. In addition to nuclear facilities, the subjects addressed include urban and rural infrastructure, communications, and agriculture and bioterrorism. Thus, this presentation will be placed in that broader context.

For obvious reasons, securing nuclear facilities is not just one nation's problem but a worldwide concern. Basically there are two kinds of facilities—nuclear fuel-cycle facilities and facilities for nonpower applications. Concerns common to both kinds of facilities relate to terrorist groups getting access to nuclear materials and using them to fabricate nuclear explosive or radiological dispersal devices (RDDs, or dirty bombs), or plotting sabotage of nuclear fuel-cycle facilities to release radioactivity in the public domain. The latter could result in great devastation, unimaginable panic, and considerable economic penalty. The experts and the stakeholders in the international nuclear community need to take a multicountry approach to adequately address these common concerns.

NUCLEAR FUEL-CYCLE AND NONPOWER APPLICATIONS

In India, nuclear power plants and all nuclear fuel-cycle facilities have been funded, developed, constructed, operated, and managed directly by the government or by public-sector enterprises under government control. Experts in developing countries generally view this as a feature that has served well in assuring safety and security. From inception, Indian nuclear facilities have been provided with physical protection measures, such as well-guarded exclusion and sterilization zones and secondary control rooms. They also have independent, redundant, and diverse safety systems, such as multiple containment, that can withstand seismic activity. These features were built to ensure nuclear reactor safety and to protect the public at large in case of an accident or incident.

It is fortunate that these robust systems, built on the concept of in-depth defense, provide some level of protection against terrorist attacks. It is necessary periodically to verify the adequacy of security in certain vulnerable areas by analysis and taking into consideration evolving design-basis threats. There is, however, a consensus among the members of the nuclear community that nuclear facilities have robust safety and security systems in place.

An examination of various safety guides and codes reveals that insufficient attention has been paid to ensuring the security of radioactive sources. Radioactive sources are highly vulnerable, especially considering the fact that terrorist access to them would endanger global security. International Atomic Energy Agency (IAEA) data on illicit trafficking in nuclear material highlights the need to further tighten controls at all points, including at international boundaries. Regrettably, confidence in the safety and security of nuclear fuel-cycle facilities does not seem to translate to the nonpower use of radioactive sources, such as in applications in hospitals, industries, and agriculture. The nonpower use of radioactive sources is so widespread and the variety and numbers of sources used is so large that ensuring safety and security will be a stupendous task. This is an area that requires much greater attention and control.

In India an independent organization called the Atomic Energy Regulatory Board (AERB) is responsible for monitoring and controlling the civilian use of radioactive sources, and ensuring their security. There is an elaborate registration process to authorize, track, and monitor sources to ensure their safety and security. The AERB has also sought and received help from technical personnel in far-flung national laboratories and state units. These persons help to identify and monitor locations where radioactive materials are in use.

Returning briefly to power plants, the systems and safety procedures in vogue, explained earlier, adopt internationally accepted design standards. Moreover, the procedures established for dealing with and reporting unusual safety-related occurrences, incidents, and accidents, and grouping them under various scales of severity are all well defined, established, and practiced meticulously. Global power plant operating groups exchange information on best practices. In contrast, there are no comparable institutional systems in place to deal with millions of radioactive sources that are used in civilian applications around the world. Reports indicate the presence of many orphaned sources. The need to secure and account for all radioactive sources from cradle to grave is of paramount importance. The need to ensure absolute control over such materials grows out of a concern not only for the health and safety of the public but also for the great risk of terrorists gaining access to them. The potential issue of dirty bombs is rather scary. While nuclear power plant security warrants attention and concern, we should not lose sight of the economic and cleanup costs and panic that could result from the detonation of dirty bombs that mix radiation sources with conventional explosives to spread radioactivity.

Physical protection plays an important role in ensuring the security of nuclear materials and facilities. The IAEA has played an active role in the development of codes, specifications, and operational procedures that deal in detail with the technical, regulatory, and licensing aspects of nuclear security. It has also conducted emergency drills. There is a need to draw up a national design-basis threat plan in line with the recommendations of the international guidelines and device security systems. Not only

will this ensure a high level of early detection, it will also delay terrorist actions by putting suitable barriers in place. Finally, an effective response will help neutralize the threat. A well-rehearsed emergency preparedness plan for nuclear power plants already exists. In fact, such a plan must be in place before a nuclear power plant goes into operation. Since effective implementation of emergency preparedness plans is the ultimate protection in emergent situations, these should be subject to periodic reviews by regulatory authorities, and drills should be conducted to expose and help address weaknesses.

The interface issues occurring between safety and security are an emerging area that requires attention. While attention has been paid to safety systems ever since nuclear energy applications were first used, security concerns per se have assumed greater importance after the September 11, 2001, terrorist attacks. Security- and safety-related issues cannot be separated. A great deal of attention should be paid to the interface between safety and security. There are situations where safety may require a particular type of plant design that may not be conducive to good security and vice versa. There are several examples of security and safety considerations coming into conflict. Access to an auxiliary control room that is established as a backup for the main control room is one example. Although the ease of movement of personnel between the two control rooms is essential while dealing with emergencies, this may pose a problem in ensuring security. Such redundant provisions necessarily demand proper analysis of safety and related security issues to ensure the best possible solution.

Security essentially has two parts: (1) managing security by the number of guards, access systems, and the like, and (2) using technology to enhance the capabilities. The regulatory agencies internationally will have to be motivated to look at the technical aspects of security in such a way that they complement and ensure effective management of the overall security of nuclear facilities. The same applies to safety culture.

The safety and security of nuclear power plants and facilities are of universal concern, and international cooperation is of paramount importance. Some of the research areas for international cooperation relating to security, safety, and their interface are listed in Box 8-1. Countries such as the United States that have experience in these areas and have mastered technologies essential for ensuring security should freely share them without any restrictions. Unrestricted dissemination of information and technology in areas relating to safety and security is essential. This is possible only through strong international cooperation. India has certain strengths that can complement these efforts in such areas as computer modeling and system design analysis tools.

The Indian Atomic Energy Regulatory Board has set up an independent entity, the Safety Research Institute, to undertake research on safety issues. Being an independent unit, it retains certain flexibility promoting international cooperation in all areas of common interest and concern. There have been good interactions between the Safety Research Institute and the Nuclear Regulatory Commission in the United States.

Organizations such as the IAEA, the CANDU Owners Group,[45] and the World Association of Nuclear Operators can play a greater role in promoting a safety and security culture. There are more than 400 nuclear power plants and associated facilities

[45] The CANDU Owners Group Inc. is a not-for-profit organization dedicated to providing programs for cooperation, mutual assistance and exchange of information for the successful support, development, operation, maintenance and economics of CANDU technology. See: www.candu.org.

such as enrichment and reprocessing plants. Millions of radioisotopes are in use around the world. All of them need to be well protected and safely operated. This highlights the absolute necessity of proper training of a substantially greater number of personnel than is being done now. India today can boast of having created a large number of talented science and technology personnel in the five decades since its independence in 1947. The strength of this large human resource should be exploited fully and effectively in international collaborative work. For this to happen, more support for international cooperation is needed. Technologies relating to ensuring nuclear security and safety should not be subject to any control regimes. Training opportunities should not be curtailed under some pretext or the other. There should also be greater transparency in the sharing of information.

To conclude, while safety and security considerations are no doubt important at nuclear facilities, radioactive sources in nonpower applications also require comparable protection. It is not safety or security, but both, and the points of their intersection require focused attention. International cooperation in research leading to advanced safety- and security-related technologies should be encouraged, and technology control regimes should not become a barrier to such efforts. In an era of outsourcing, India, with a large pool of talented and competent science and technology personnel, could play a significant part in the global effort of ensuring the safety and security of nuclear installations.

Box 8-1
Research in Security Technologies

General Type of Technology	Specific Type of Technology
Sensors	Imaging Sensors: Infrared, multispectral, nonintrusive millimeter wave, and behind wall imaging
	Intrusion Sensors: all-weather and all-terrain, economical sensors with a very low incidence of false and nuisance alarms
	Contraband Detection Sensors: personnel, baggage, and vehicles for explosives and metal (e.g., weapons)
	Radiation and Nuclear Material Sensors
Surveillance	Personnel Access Control: Biometrics (positive identification)
	Alarm Assessment: Automatic alarm assessment with intruder characteristics (e.g., number, arms, and direction of travel)
	All-weather day-night surveillance
	Robotics: automated, remote-controlled vehicles and group intelligent, mobile machines that carry out specific tasks (e.g., detection and deactivation of explosives,

	chemical and biological agents)
	Computer modeling and simulation
	System design and analysis tools
Research in Safety	Safety-related technologies
	Computer modeling, simulation, and analysis of willful malevolent acts that raise safety concerns
	Root-cause analysis: design implications and social dynamics
	Safety and security culture

9

Discussion of Protecting Nuclear Facilities

G.R. Srinivasan and Rose Gottemoeller,
Discussion Moderators

Session chair V.S. Ramamurthy framed the discussion by noting that new technologies offered opportunities for constructive as well as destructive use and that atavistic attitudes still exist, both in the West and in India. Nuclear technology, more than 50 years old, is a mature technology. It went through a phase of very rapid growth, followed by one of concerns about safety, and then a phase in which proliferation was the major concern; now it has entered a phase dominated by security concerns rising from terrorist threats.

The nuclear industry has addressed these issues in various degrees at various times; perhaps it is the only industry where this is done, but Ramamurthy reminded the group that all new technologies go through these phases. This is true now of biotechnology, the chemical industry, cloning, and other technologies—the similarities cannot be missed. Whatever we do today in the realm of nuclear technology might be a lesson on how to handle the emerging technologies of tomorrow; the issues are not going to be very different. Thus, he urged participants not only to address concerns surrounding nuclear facilities but also to address other emerging technologies.

G.R. Srinivasan noted that both presentations discussed the three real problems of terrorism confronting the nuclear industry: (1) dirty bombs, (2) nuclear explosives, and (3) sabotage or malevolent acts against nuclear facilities. He added that these three threats stem from the unauthorized removal of material as well as sabotage on nuclear plants, both with or without insider assistance, and agreed with John Holdren's view that sabotage has been neglected. Srinivasan also suggested that one point raised by P. Rama Rao had to be emphasized again: nuclear power plants have a built-in policy of defense in depth, a policy of redundancy, which would stand in good stead against terrorist attacks. Thus, our concern about the catastrophic destruction of a nuclear power plant should be limited to one or two design-based threats (DBTs). In most other cases it would not be so serious. Citing Rama Rao, Srinivasan noted several built-in features of a nuclear plant that could save the situation for the plant; we often jokingly reminded visitors in the

control room not to sneeze heavily lest, because of the fail-safe mechanisms, the reactor is shut down. This is the type of defense in depth or bias towards safety that is built in.

Suggesting that Holdren's paper could serve as an action document about the steps that can be taken to reduce future risk, Srinivasan elaborated on the design of safety systems and redundant systems. At first these systems were designed for a few incidents, such as a jet of water coming out. Then, after a few fire incidents, the spacing between redundant systems was adjusted for fire. Now we must incorporate threats from explosives and sabotage into the DBT, so there is reason to redesign the safety systems.

Additionally, Srinivasan noted that international cooperation on nuclear safety is very important, and while there may be proprietary details to worry about, these can always be addressed. He was particularly pleased that Holdren had specifically emphasized cooperation with India.

When Srinivasan was Vice-Chairman of the Atomic Energy Regulatory Board there was fairly satisfactory control over the regimented areas, such as nuclear power plants and nuclear facilities, but for the nonregimented areas, such as radioactive sources and the materials necessary for a dirty bomb, there were many areas in need of greater security. This is the situation in many other countries, and there is a real dearth of information in this area.

Security considerations should be included from the beginning—they cannot be retrofitted—and security-related training is critical; the nuclear industry is a knowledge-driven industry and safe operation requires training. Nuclear safety-related training would be strengthened by international cooperation and an exchange of experience.

The DBTs for nuclear power plants are useful in fighting terrorism, as these are state-of-the-art. They include safeguard systems, physical protection systems, extensive data mining (required to fight terrorism), and advanced tools for analysis of design-basis threats such as codes and computer models. In fact, even the response and the delay and modeling of the physical protection system is run through software programs. So any upgrade required has a considerable science and technology component for security-related concerns.

Srinivasan also emphasized that the nuclear industry should not be shut down because of terrorists and their activities; this amounts to punishing the victim, not the aggressor. As for energy supply, he noted, diversity of energy supply equals security.

Srinivasan concluded his comments by reemphasizing a point made by both speakers: that nuclear security is a comprehensive, top-to-bottom, multidimensional, multidisciplinary, multiorganizational effort, not a matter of pointing at one particular area. Production, safety, and security objectives have to be simultaneously achieved. Security is an area where a small security staff of 50 or 80 people cannot tackle the problem. In a nuclear power station everyone needs to be involved with security. Security culture has to be embedded in the organization itself and all four or five hundred employees. It is important that each person does the right thing even when no one is looking.

Discussion moderator Rose Gottemoeller observed that no country owned the perfect model for security. Instead, the best practices of each country can contribute to improving worldwide performance in this area. International cooperation is vitally important because of the driving need to improve the security of the entire system of nuclear material and facility protection worldwide in the face of the urgent threat of

international terrorism. By learning the best that each country has to offer, we can all improve our efforts; this process is not only vital but also timely for each country with civilian or military nuclear facilities or both. We all have the same problem to address—the threat of nuclear terrorism, and we all want to do the best we can to prevent nuclear catastrophes and to protect and preserve our national nuclear assets.

Gottemoeller stated that her assessment was drawn from long experience working in the U.S.-Russian context. In the U.S.-Russian environment, cooperation seemed to work best under the following conditions.

First, the relationship is treated as a partnership, not a relationship wherein one country is providing assistance to another country.

Second, each country is considered to have best practices in nuclear material and facility protection to be incorporated into joint projects. These measures can also inform the counterpart country's own protection efforts.

Third, the partners each bring resources to the table, whether financial, technical, or human. It is important to underscore that it is not necessary for the resources to be financial for a full partnership to emerge. We have found, for example, that Russian monitoring and sensor systems are sometimes more robust for operating in the harsh climate of the Arctic than U.S.-developed systems, and we had to learn this lesson. Americans had to learn to examine such possibilities rather than to assume that their own systems and technologies were best.

Fourth, each partner participates in project management and decision making. There should be a well-developed system of sharing information and coordinating activities. Such a system performed very well in the early days of the U.S.-Russian cooperation on nuclear reactor safety, but it has not always been present in other types of cooperation, such as the material protection, control, and accounting program.

Fifth, an all-or-nothing approach is generally not helpful to the cooperation; that is, demanding all facilities of a certain type be thrown open for joint project work. Instead, we have found that a pilot project approach is useful, focusing on a single facility to begin with, building up mutual confidence in the cooperation, and then perhaps in the future, on the basis of mutually arrived at decisions, expanding into a wider array of facilities.

Finally, the use of indigenous manufacturers and construction firms can speed cooperative projects and help sustain them. Early on, and again this was another U.S. mistake in establishing the cooperation with Russia, we insisted that U.S. products and companies be used. We were trying to sell the cooperation politically to the U.S. Congress. This approach led to many problems. Russian colleagues resisted this and resented this position. Further, this created difficulties with the sustainability of the joint project efforts. Joint projects today make wide use of Russian firms both for equipment and for construction services. This was a very important lesson from the overall cooperation.

These examples deserve examination and should inform broader international cooperation on protection of nuclear materials and facilities. There is no need to repeat the mistakes of the U.S.-Russian relationship, but rather we can move more quickly to effective cooperation.

Gottemoeller concluded by asking how the problem of radiological dispersal devices (RDDs) can be further examined, and noted that there is a U.S.-Russian bilateral

initiative examining the question of RDDs and nuclear sources, and trying to establish priorities in addressing the problem of control, protection, and accounting of sources.

S. Rajagopal noted that nuclear risks are not the same across-the-board as is seen in the example of reprocessing. As Holdren explained, the risks of attack and release of a large quantity of cesium-137 depends on whether the reprocessing plants are centralized and whether there is a large inventory of spent fuel. This is not so in India because reprocessing plants are decentralized in India. So you can see the risks are fewer when compared with the French facility at La Hague, where there are thousands and thousands of tons of spent fuel kept in the pool. Because of U.S. policy—fuel is not reprocessed but rather goes through a once-through cycle—the United States is holding very large stocks of spent fuel. It then becomes necessary to store this spent fuel away from the reactor. We do not have any away-from-reactor storage except perhaps in Tarapur, because of the policy that we cannot reprocess U.S. fuel.

The risks of illicit trafficking in nuclear (especially fissile) material are also variable, but because of the degree of illicit nuclear trafficking reported by the International Atomic Energy Agency, we need to take this threat very seriously now. Rajagopal was not sure that a terrorist who looks for spectacular results and wants to create instantaneous panic and human loss would resort to a dirty bomb.

As for a terrorist attack on a nuclear plant, what is important is a well-rehearsed emergency preparedness plan that considers the worst-case scenario, looking at wind direction, the radioactive transport mechanism, and so forth. With a very well rehearsed emergency preparedness plan, we will be able to mitigate the effects quite effectively, irrespective of whether there is an accident in the plant or a terrorist attack.

Richard Garwin noted that when he was a member (with Lewis Branscomb) of the National Academies' group that wrote *Making the Nation Safer,*[46] they looked at the security of radioactive sources. The United States really needs an inventory and more frequent reporting of where the sources are located in order to minimize their use in radiological dispersal devices.

Garwin's view was that the biggest threat is not an attack on a nuclear facility, (for example, power reactors or reprocessing plants) at least not in the United States, but on spent-fuel storage systems. When prioritizing risks, the spent-fuel casks have received a lot of attention, but they are not that large a problem compared with the storage pools for spent fuel. Storage pools are a greater problem, because they are not as well protected as the reactors themselves, and of course, reactors can be a big problem. The terrorists—if there is a concerted terrorist attack on a reactor—are much better motivated, better equipped, and more interested in their job than are the guards who defend. The terrorists can use tear gas at the same time that they use rifles, machine guns, automatic weapons, bazookas, and all kinds of weapons that can be carried in an attack. Unless we actually look at what can be done and at the difference between security and safety, as Rama Rao indicated, we do not get the right evaluation of the threat to the reactor. The difference between security and safety is that the terrorists can choose to attack the worst plant during the most favorable weather conditions for maximum damage. They can intentionally attack the specific redundant systems to destroy them at the same time,

[46] National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, D.C. The report is available in PDF format at *http://books.nap.edu/hml/stct/index.html*.

whereas safety imagines that they are destroyed either through some common mode or through a simultaneous accident. So if, in the context of U.S.-Indian cooperation, we do not want to particularly look in detail at Indian plants, U.S. experts could at least use Indian experts' help in evaluating the threat to U.S. plants because it is not going to benefit the worldwide nuclear industry to have a terrorist-induced catastrophe in any country.

Regarding the Sellafield facility in the United Kingdom, there are more than a thousand cubic meters of liquid fission products, containing 30 times as much cesium-137 as did reactor number 4 at Chernobyl. Furthermore, although there is much less thermal driving force than in the fresh spent fuel within the reactor, if it is struck down, there is plenty of power generated to boil those tanks and to burst them or to evaporate the cesium-137. We must install filters that will accumulate the evaporating cesium-137 in thousands of tons, with improvised filtering material in order to compensate for an attack. These are, Garwin concluded, very serious problems, that could lead to a disaster unless they are carefully evaluated, not from our perspective, but from that of a terrorist's choice of time and place.

This point was seconded by Kumar Patel, who noted that threat perception may change daily, and since the initiative lies with the terrorists, they have an option to choose when and where to attack. This means that security is not a linear function of the number of armed security guards at a facility. It does not depend on the amount of equipment that is installed, nor does it move linearly with the sophistication of the equipment. Security has to be incorporated into the professional culture of those who work in all facets of the nuclear industry.

B. Raman posed a number of questions regarding physical barriers, the role of intelligence, air attacks on nuclear facilities, and other kinds of attacks.

Holdren's response was that regarding barriers, there are a number of possibilities, some of them examined in *Making the Nation Safer*. Towers and cables in various arrangements could make it much more difficult for an aircraft to strike a reactor containment vessel at the right angle, at the right speed, or at all, depending on how towers and cables were deployed. One idea that appeared in the German press for countering this possibility would be to use dispensers that can throw up an obscuring fog if a reactor is under attack, so that the operators of an aircraft could not see where they were going, and could not accurately see their target. It should be noted that for an aircraft attack against a reactor to be effective, a number of conditions have to be met, including a very precise strike against the reactor. If one cannot see where the precise target is, this becomes very difficult. It has already been widely pointed out in the aftermath of September 11, 2001, that flying a jumbo jet into a skyscraper where the attacker does not care where in the building the strikes occur—it does not matter whether the 70th floor or the 80th floor or the 60th floor is hit—is much easier than flying an airliner into a specific point on the ground. This was already demonstrated in a way when the aircraft that was aiming to strike the Pentagon actually struck the parking lot. It then skidded into the Pentagon and caused a lot of damage, but it underlines the point that flying to a particular target on the ground is quite difficult, and you can make it more difficult with barriers, obscuration, and perhaps with other means.

Regarding the role of intelligence, Holdren agreed that, of course, intelligence can play a major role in intervening in terrorist attacks of all kinds, including attacks on

nuclear facilities, and that the growth of international and national cooperative efforts to deal with terrorist threats could, in general, be effective in the context of attacks on nuclear reactors. In the United States, the Nuclear Regulatory Commission (NRC) has greatly increased its interaction with other federal agencies that have security responsibilities, and there is far more communication between the NRC, the Department of Energy, the Federal Bureau of the Investigation (FBI), and the Department of Homeland Security. This extends beyond intelligence to response capacities, that is, in thinking about how to respond to an attack on a nuclear reactor. The capacity to engage multiple agencies very quickly in an emergency response is now being developed.

Finally, on the question of armed intruders versus other threats to nuclear reactors, Holdren elaborated that the threats involve permutations of combinations of intruders and insiders—some might be entirely intruders and some might be entirely insiders. A case where there is someone already inside the reactor as part of the staff or as part of a maintenance contingent could very well do a great deal of damage if such a person were able to smuggle in explosives or were particularly knowledgeable about the plant.

In the discussion that followed, additional questions were raised, with responses by the speakers and others.

One participant asked whether space-based surveillance of nuclear power plants was possible. Garwin responded that it was most likely not possible. Terrorists know when there is cloud, and when a geosynchronous satellite would be blocked. Nuclear energy facilities are sufficiently rare that the way to survey them is from the ground, with towers, with people if need be; this is also affordable, as television cameras are now extremely small and inexpensive. Terrorists could, of course, destroy surveillance systems as part of the attack, but there could be small, covert, and inexpensive systems that would operate in any scenario.

It was also suggested that there might be "force multipliers" in nuclear facilities, the way that other civilian targets were used to increase the devastation. Branscomb responded by noting that the problem is made more severe because there are almost no statistics to suggest the appropriate model of terrorist capabilities we should have in mind. Branscomb would divide their capabilities into two parts: (1) What equipment, vehicles, weapons, devices, and other material devices and facilities they would choose to attempt an attack, and (2) to what extent would they know and understand the target and attack strategy? He submitted that not only is it inherently difficult for terrorists to launch an attack that requires the assembly of a very complex set of equipment, perhaps airplanes with shaped charge weapons, but also it exposes them to intelligence surveillance. Branscomb observed that it was known, after the fact by the FBI, that some of the terrorist groups who were involved in the September 11, 2001, attacks were also involved in trying to obtain experience in how to fly crop-duster aircraft, clearly with a biological or chemical attack in mind. Unfortunately, it was not communicated properly. So there was a catastrophic risk that the terrorists would be discovered. He concluded, from what he agreed was an oversimplified view, that it is safe to assume that terrorists would seek a strategy in which the materials they need to acquire are broadly available, undetectable, and as easy to acquire as possible. Branscomb did not see any limitation on the level of terrorist knowledge or expertise and asserted that there is still a question as to whether Osama bin Laden's previous experience as an engineer informed al Qaeda's attack on the World Trade Center buildings. They did try, and failed, in 1993, and they

had 7 or 8 years to try to figure out how to do that job successfully. Branscomb said that he would not be surprised if, in fact, they had a model for how to bring the towers down that involved quite sophisticated analysis that they could do in the privacy of their own secure locations. So, these conjectures about equipment and expertise may provide a useful guide to avoiding what otherwise might be criticized for assuming the worst-case scenarios. Certainly, for many years our military has planned against the worst-case scenarios. We spent a great deal of money on our military when in fact our assumed enemy, the Soviet Union, did not have the capabilities our worst-case scenario imagined they might have. Today, the correct worst case to assume is that terrorists have a lot of technical knowledge, but perhaps not a sophisticated array of equipment and facilities.

Both Holdren and Rama Rao were asked to comment on legal issues related to the protection of nuclear facilities in their respective countries. Are laws updated in light of technological improvements or in light of new threats to nuclear facilities? Holdren responded that in the United States there is a discrepancy in U.S. law because federal authority that applies to nuclear weapons does not always apply to nuclear power plants: nuclear power plants were not thought of historically as a weapon that someone might use against the United States. So the situation now is that nuclear power plants are not ordinarily guarded by employees of the federal government, but are guarded by private employees who are not entitled in most states to use automatic weapons. There are also legal questions about their capacity to use deadly force in defense of private property.

Holdren thought that the NRC's own view is that U.S. law is currently inadequate for this complex of problems. The NRC has requested that Congress change the law in order to bring about a more coherent, uniform, and effective system for protection of nuclear energy facilities. So far this has not happened. Richard Meserve, a former NRC chairman, visited some state legislatures, including the Massachusetts legislature, and tried to persuade them to change the law state by state. He has been unsuccessful. Holdren's overall views and those of many people responsible for improving the situation in the United States is that the law is currently inadequate.

Rama Rao noted that the situation in India was just as inadequate as in the United States. There is no strong connection between national legislation and regulations and the Atomic Energy Regulatory Board. However, a study, *State System of Physical Protection in India*, was conducted and as a result there is a greater awareness of the problem.[47] There is a need to base the security of nuclear energy facilities in law. Rama Rao noted that rules can be as effective as laws, and in the current situation the loss of nuclear material would be treated as would a theft of any other material, punishable under law. Regarding defense research, threat perceptions are analyzed in depth and we have not had a grave incident, but this was not so for civilian facilities. Another Indian participant noted that in the last 2 or 3 years, there were concerted efforts to examine threats to civil nuclear facilities and nearly 250 design-basis threats were drawn up; India has improved in the last 3 years, but a lot more has to be done.

Finally, Gottemoeller noted that technology control was another way of addressing the threat of large-scale terrorism. Technology controls and export controls are an important tool in our toolbox, and they have a good practical effect, as

[47] In 2006, new legislation was introduced in the Indian parliament, which will create a separate, law-based regulatory board for India's civilian nuclear facilities.

demonstrated by Iraq. A major Carnegie Endowment International Peace (CEIP) study[48] examines the evidence of Iraqi weapons of mass destruction and the decision to go to war by the George W. Bush administration. A key conclusion of that study was that there was a very positive impact on constraining the ability of Saddam Hussein's attempt to reconstitute his weapons program through the use of technology and export controls throughout the 1990s.

That said, Gottemoeller agreed with the view that technology control should not be a barrier to safety and security cooperative endeavors. The conclusion of a small working group of eminent experts convened in 2003 by CEIP was that indeed the legal authority for security and safety cooperation was already in place and there should be no barrier to pursuing such cooperation. However, she added, this opinion was not fully accepted by some of those inside government, and she expressed the hope that this will be an area where there can be very wide ranging cooperation between India and the United States.

Kumar Patel concluded the discussion by observing that while there are broad differences of opinion on the real threats to nuclear power plants and nuclear facilities, one significant incident could have enormous social and physical consequences; there would be nuclear fallout, but also societal fallout, which may make nuclear power plants undesirable all over the world. This is a very significant issue and requires greater thought. As Branscomb noted, the threats will come from smart people using commonly available materials. We need to focus on how we deal with the problem of protecting nuclear facilities from both inside and outside threats.

[48] Cirincione, Joseph, Jessica T. Matthews and George Perkovich. 2004. *WMD in Iraq. Evidence and Implications*, Carnegie Endowment for International Peace, Washington, D.C.

10

Local Realities of Terrorist Threats

Julio Ribeiro

India has been afflicted by terrorism for many, many years. The most important and most significant experience that India has had with terrorism was in Punjab in the 1980s. I personally experienced this terrorism; there were two attempts on my life, one in Punjab itself when I was director-general of police and one in Bucharest when I was ambassador to Romania. I shall start with the former attempt, not because I want to highlight it; rather, I want to relate it to the question of how science and technology could have helped in preventing these attacks, although regrettably, it may also not seem as if it could have helped.

In Punjab, shortly after I took charge as director-general of police, Rajiv Gandhi, our young and dynamic prime minister, told me to take "Black Cats" with me. These are specialized security agents that operate in Delhi. Important leaders in India have Black Cats to protect them. I responded by saying, "Look, I am a quasi-military man. I belong to a uniformed armed service. I can't possibly be protected by somebody else from some other service. I have to be protected by my own men. If I cannot command their respect, that's it. I don't think I would be able to function."

Soon thereafter I was on my usual early morning walk with my wife around the police officers' compound when we heard the sound of weapons firing. I lay down on the ground pretending I had been shot. The attackers thought that I had been shot. They had shot 49 rounds from AK-47s and self-loading rifles into the building and the walls but fortunately they did not hit me. The attackers used a vehicle that they had painted so that it would appear to be a police jeep; they had replicated the color and markings. When the attackers came in, the police guards at the door, who were part of my security detail, saluted them because one of the men sitting in front was wearing the uniform of a police inspector, another in the back seat was dressed as a head constable, and the others were dressed as constables. The guards let them go through. The very next moment the attackers called out to the other guards who were near me and said, "We want to inspect your weapons." When the guards showed them their weapons, the intruders started firing and killed the guards. I heard the sounds of the guards being killed and that saved me.

How could science and technology have helped to save me? I do not know. If there had been some way to detect that these men were not regular policemen, perhaps the crisis could have been avoided, but I cannot imagine how that could have been done.

The assassination attempt in Bucharest was different. Rajiv Gandhi told me that it was a safe place for me to be because Nicolae Ceausescu was ruling Romania and he did not allow dissent or terrorism. Thus, I went to Bucharest. Very soon after that, Ceausescu and his wife were both killed. While I was going for a walk, again with my wife, they jumped out of a car and started firing, and I knew that they had come for me again. I was 62 years old, and my attackers were 26 years old. I ran faster than they did and that is why I survived.

Again, in this instance, I do not think science and technology could have helped me. I do not know if it could have helped the Romanians in preventing my attackers. The attackers probably paid a bribe to enter the country—it was not easy to enter Romania, and yet they did.

My story about Punjab builds upon my stories about the attacks that I experienced. Punjab is one of the more prosperous states in India. I think Punjab deserves to be so because its people are very hard working. They want to improve their quality of life. If they have a bicycle, they want a motorcycle. If they have a motorcycle, they want a jeep. If they have a jeep, they want a car. However, prosperity spawns other problems. Not everybody in Punjab is prosperous. In addition, there were political reasons for terrorism beginning in that state. There were others who joined terrorist groups because they were criminals. The terrorists attacked certain police outposts. The policemen in the rural areas of India are not very alert, because they do not expect anyone to challenge them. Nonetheless, they were attacked and their weapons were stolen. Police weapons were used by terrorists to kill innocent people.

There was a think tank in Lahore, Pakistan, across the border from India. This think tank comprised leaders of the Sikh terrorist movement. They decided that the best way to send their message to the Indian government was to attack the Hindu community in Punjab so that the Hindus would leave the state, and that would ensure their victory. They demanded a separate state even though 99 percent of the Sikhs did not want this. Nevertheless, 1 percent, or less than 1 percent, decided that a separate state was their goal and the only way to achieve that was through terrorism. They could not achieve it by regular warfare because they did not have the wherewithal. Having decided that they would frighten the Hindus, the Sikh terrorists attacked them in the villages where they lived. (Very few Hindus lived in villages.) In many places they were shot for no other reason than their religious affiliation. As a result, the Hindus left; they moved to Delhi and other places. Some of them came to the bigger towns of Punjab, Jalandhar, and Ludhiana.

What happened to the people? The Hindu community began to demand more security. As their demands increased, the Indian government started sending increasing numbers of paramilitary forces. In response, the Sikh terrorists struck at easier targets and at targets that people did not expect them to hit, including buses, trains, marketplaces, and places where Hindus congregated for religious purposes, called jaagarans, at night. The terrorists pulled people off of buses and separated the women, whom they did not

touch. They separated the men with beards because all Sikhs are supposed to wear beards and turbans, and then they lined up the men without beards and turbans and shot them, even those who were Sikhs.

People across the border helped the Sikh terrorists acquire more sophisticated weapons, namely AK-47s. After the war in Afghanistan, many weapons were available in the bazaars of Peshawar and different parts of Pakistan. These weapons came into Punjab and they were used by terrorists.

The police reacted by demanding AK-47s for themselves, which was more of a psychological demand. I asked them, "What are you going to do with the AK-47s? AK-47s could be good for terrorists, but what will you do with them? The AK-47 is a weapon that covers a large area; if you fire, you might kill innocent people. The terrorists might escape, but others would be shot." My arguments did not register with the police. This kind of demand had to be met in order to raise the morale of the police. As a result, we purchased AK-47s for them.

I have described the type of terrorism we are facing. I wanted to relate it to science and technology, but I do not know exactly how to do that. AK-47s are a product of science and technology, but they are now outdated. The police wanted more sophisticated weapons. I personally did not think that the police needed them. Better intelligence is a more effective tool. I must mention that when I was attacked in Bucharest, the intelligence agencies had already warned me to be watchful. They even told me the names of my suspected attackers. I did not know who they were, but they were the persons who attacked me. I do not know how intelligence officers got this information. After I received the warning, I stayed home for 20 days, but after that it was difficult to continue staying at home. On the first day that I went out, I was attacked. In my opinion, our intelligence agencies were doing a very good job, but there were more and more demands on them to produce more information that would help us fight the type of terrorism we were facing.

Of course, we never thought about science and technology. We made no demands on our scientists and technology experts because we did not know that there were ways they could help us in such circumstances. The scenarios that our U.S. friends have discussed fortunately have not occurred in our country yet. In that respect we are many years behind, and I hope that we remain so as far as terrorism is concerned. The United States faces particular threats that India does not yet face. For instance, I do not think that an attack on nuclear facilities has ever entered our minds or those of terrorists. I do not know where they would be able to get this type of material.

I must also mention that I had not experienced terrorism until I went to Punjab in 1986. Before that, I did regular policing in my own state, Maharashtra. I was the police commissioner of Bombay (now Mumbai). There we had many problems with the underworld but certainly not with terrorism as such. Terrorism was a new phenomenon that I learned about in Punjab. Much later, when I returned from Bucharest, I read about the first terrorist attack in my native city of Mumbai.

Corruption is another closely related problem facing India. A specific case in which terrorism and corruption were linked was the illegal importation of RDX-based explosives,[49] facilitated by bribes, and the subsequent detonation of those explosives in attacks on the Air India building in Bombay and the Bombay Stock Exchange. These

[49] The full name of this explosive is: cyclotrimethylenetrinitramine.

attacks killed more than 200 people. In this case it does not appear that police knew about the illegal import of explosives until after the explosions.

There were social consequences of this terrorist act. We had to think about this type of terrorism coming into the big cities of India. We have had similar terrorist strikes in the city more recently, in 2001, 2002, and 2003. In each of these instances, explosives were placed on the last seat of a bus. The first incident did not generate significant attention. After an interval of time, the terrorists did the same thing, which meant that the police had relaxed. What can science and technology do to detect terrorist strikes of this nature? Islamic terrorists succeeded in putting explosives under the last seat of buses and caused enormous damage. They cause less damage than the big RDX explosions, but it was certainly enough to cause further rifts between the local communities.

Although we often hear about Islamic terrorism, this term is a misnomer because Islam as such does not teach anyone to be a terrorist. I do not think that any religion tells a follower to kill others in the name of God. I have gone to the poorer areas of Bombay to talk about the concept of Umma (the concept of Muslim brotherhood worldwide) and the concept of jihad. These concepts have been misrepresented by fanatics to lure people into committing terrorist acts. These misrepresentations have to be addressed by the community itself. From my experience in Punjab, I believe that although we must go after terrorists who kill innocent people, that alone is not going to help. Individual terrorists are immediately replaced by someone else. New ones will be recruited as long as they feel that terrorism will provide them with what they desire. As long as this happens, the authorities are not going to stop these acts of terrorism. Many terrorists have been drawn into this vortex by feelings that Islam is in danger, and that Christians and Hindus are threatening their way of life and they must defend themselves; that is, they have to strike in order to survive.

This is unfortunate. The only way that this view can be countered is to win the hearts and minds of the community that has been affected. In Punjab, although a lot of people take credit for having stopped terrorism, I really do not think it would have stopped unless the people themselves decided they did not want it anymore. Until people reach such a decision, terrorists are going to continue to attack because they depend on the support, covert or overt, of their own community. When that support ends, terrorism is then brought to an end. For example, in Punjab when the depredations of terrorists became worse than those of the police and security forces, the people decided that they would no longer condone terrorist actions, and they gave information to the authorities that led to the elimination of the terrorists.

In conclusion, terrorists and terrorism are two different things. You have to go after the terrorists, but terrorism can be fought only if you win the hearts and minds of the people involved.

After the Gujarat riots we went to the main slums of Bombay. I went to Dharavi, considered to be the biggest slum in Asia, and met with the women. We should work with women because they have great influence over their male relatives. It is very important to talk to the women and to ask them for their support in our fight against this type of communalism.

What we did was ask women to state what they had experienced in 1992 and 1993, when there were big communal riots in Bombay in which people, mainly Muslims, were killed. The women told us that they had all suffered. We asked, “Did you support

your men when they went out to fight?" Some of them admitted that they did. They said they were not going to do it anymore because the children suffered—they did not go to school, they did not get milk to drink, and some of them did not have enough to eat. There was a curfew, and many of the women suffered.

Later, we brought religious leaders, particularly from the army, to meet with the women. The Indian army has religious leaders based in Poona, whom we asked to talk to the women. The religious leaders said, "Look, here is a message that can be given. There is no point in killing somebody because he worships God in some other way by some other name."

We must take similar initiatives if we are to make any inroads into the Muslim community, which is under attack today. The Muslim community is under great constraints. The constraints are not only from Hindu fanatics but also from their own fanatics. Fanatics have to be isolated. Once they are isolated, terrorism is bound to suffer and to be brought under control.

I am interested in learning how science and technology can help reduce or eliminate terrorism. For example, policemen used to be assigned the task of providing airport security, but they were not interested in that work. Now another organization is charged with airport security, and it is doing a much better job. I hope that this continues because there have been a number of hijacking incidents, including in Kathmandu and Punjab. Perhaps there are innovations that can help in detecting weapons that are used to hijack airplanes.

Contraband-detection sensors, personal access control by biometrics, and other innovations mentioned by our U.S. friends might be useful when the level of terrorism increases in India. We have not yet experienced that level of terrorism. I feel that we should be prepared for it and gain from whatever the Americans share with us and whatever help they can give us.

11

Securing Against Infrastructure Terrorism

Lawrence T. Papay

The two words in the title of this paper that are particularly important are "infrastructure" and "securing" or "security." Each will be examined in turn.

What is infrastructure? Infrastructure includes all of the things we find around us on a day-to-day basis—buildings, roads, and highways as well as systems for water supply, sewage, electric power, oil, gas and communications. Attacks against a particular society will differ based on the level of technology employed by that society. In a rural society, the threat is generally of a more personal nature, since the attack is on a local level. In contrast, what we saw on September 11, 2001, was a highly visible terrorist act, perpetrated on a technologically advanced society with a degree of sophistication (commercial airliners used as "cruise missiles"), that was commensurate with the nature of the target.

Now, let us examine security. First, although science and technology will not solve all problems related to terrorism against the components making up a modern regional or national infrastructure, it can help in prevention, mitigation, and restoration if an attack or attacks are attempted or carried out. In other words, science and technology will help to reduce the threat of terrorism, but it cannot eliminate it. Unfortunately, terrorism has become a fact of life. Whenever there are dissatisfied people who are willing to give up their own lives or do not value human life, it will be difficult to eliminate the threat of terrorist attacks.

A specific point where science and technology can help is in the area of intelligence, by providing information about the potential for an act of terrorism to be conducted. For example, what is being done to sort through open-air communications—both e-mail and voice wireless—is rather startling both in quantity and in degree of sophistication. There are programs, such as Trailblazer at the National Security Agency, that look for keywords and matches. Some of the recent terrorism alerts have been based on information gathered through these programs.

There is another aspect that inexorably links infrastructure and security. The more sophisticated, complicated, or technologically evolved the infrastructure, that is, the more fragile it is, the more difficult it is to secure against terrorism and the greater the

need for science and technology solutions. The latter was the particular challenge that we were confronted with at the National Academies in producing the report entitled *Making the Nation Safer*.[50] What can and should be done incrementally as society becomes more and more complex, sophisticated, and interdependent? How do you establish layers of protection because of increased vulnerability?

This paper will look at vulnerabilities, cost-effective science and technology strategies to affect the threat of attack, the various steps we would encounter if an attack were carried out, and possible areas of collaboration between India and the United States. For simplicity, science and technology strategies will be defined in terms of three steps in the process: prevention, mitigation, and restoration of physical infrastructure.

VULNERABILITY ASSESSMENT

First, we need to define what constitutes vulnerabilities: how should vulnerabilities be characterized and assessed? Similarly, how should the effectiveness of the terrorist's weapons be characterized and assessed?

Scale plays an important part in this analysis. On a local level, for example, at the village level, vulnerability is tied to the local community and the people who live there. Terrorist threats are played out locally, and vulnerability is measured in those terms. Straightforward and basic means of attack, such as bombs, rocket-propelled grenades, and gunmen, are used. In a more urban environment, more complex and sophisticated methods of delivery must be examined. Obviously, these methods require ways of defending against them. Urban terrorist threats are larger and more catastrophic in potential, but strangely enough, less personal in nature.

In a rural village, for example, cyberattacks are not a threat, so vulnerability is very low or nonexistent. This would be true for a significant portion of India, but not for the entire country. In Bangalore, a cyberattack or even a physical attack on local computer server farms could have a significant impact on a significant portion of the work force's ability to function, resulting in a significant impact on the local economy. Again, as a society begins to get more complex and builds up an ever more complex and interdependent infrastructure—whether information technology (IT) or communications or electric power or a combination of the three—more complex, but fragile, targets for attack increase vulnerability and risk.

The following examples illustrate the fact that the process of assessing vulnerabilities requires the exploration of a series of scenarios. Catastrophic vulnerability can be viewed in a variety of ways. Perhaps the most obvious areas of vulnerability are high-value, high-visibility, high-consequence targets. Governmental buildings, religious sites, banks, and other major facilities become symbolic targets. Just as the World Trade Center was symbolic for the United States, and perhaps internationally, in India the attacks on Parliament and on temples are also symbolic.

Vulnerability extends far beyond the lives lost and the immediate physical damage. The impact of the September 11, 2001, attacks demonstrates this. They were

[50] National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, D.C. The report is available in PDF format at *http://books.nap.edu/hml/stct/index.html*.

horrific in terms of loss of life—3,000 people from 80 countries—and the destruction of the World Trade Center and the Pentagon.

The economic impact of the September 11, 2001, attacks was felt on several levels. With the destruction of all the buildings that made up the World Trade Center, the insurance industry was assaulted on several fronts. Historically, in major catastrophic events, whether man-made or natural disasters, the economic impact has been felt by one particular insurance pool (life, casualty, liability, or property) rather than more broadly across the entire industry. The insurance costs associated with the World Trade Center event are in the range of $60 to $80 billion, and that impact is being applied against every major insurance pool.

Cutbacks in travel and tourism after the September 11, 2001, attacks have had severe effects on these industries. In fact, several airlines in the United States have gone bankrupt and others have been brought to the brink of bankruptcy.

Consequential impacts also are significant. Fear, anger, and similar emotional impacts were manifest because of the symbolic nature of the attacks on September 11, 2001. In addition, the U.S. populace has experienced an increased sense of vulnerability and loss of freedom. If someone believes that his or her daily routine has been compromised by the actions of terrorists, whether in a rural town or at an international airport, there is a sense of loss of freedom. After the September 11, 2001, attacks, people in the United States have had to adapt to the threat of terrorism as a way of life.

This threat requires that adequate tools be available to do a meaningful assessment of risk and consequences.

PHYSICAL INFRASTRUCTURE

Physical infrastructure refers to the various systems that are required to maintain our society in today's world. This paper will simply highlight broad areas of physical infrastructure with the objective of identifying basic themes that may offer opportunities for collaboration. These broad areas include energy, the civil infrastructure of cities, water and wastewater, and transportation. For convenience, the discussion of energy infrastructure will be split into two parts: electric power and hydrocarbon fuels.

Energy: Electric Power

For electric power we need to look at the entire supply and delivery system: fuel supply, generation, transmission, distribution, and the control systems involved at each of these stages. From a systems approach, electric power can be generated by nuclear power, coal, oil, gas, wind, or biomass. The use of nuclear power to generate electric power has unique aspects. An attack on any one plant in the United States, whether successful or not, would probably prompt the Nuclear Regulatory Commission to shut down all civilian nuclear power plants until the attack and the vulnerability of nuclear plants was reexamined. An attack on a nuclear power plant would also have radiological consequences.

In looking at the vulnerabilities of the electric power system, it is clear that the plants that are actual generation facilities—be they coal-fired, gas-fired, or nuclear

power—while attractive as large visible targets, are not per se major points of vulnerability. It is the disruption of the ability to deliver electric power to the end customer that causes the greatest vulnerability.[51]

The grid itself (and the control systems associated with it) is the most critical component in an electric power system. From a physical point of view within the grid, it is not the transmission towers, wires, and cables, but rather the substations that represent the greatest vulnerability. The substations, principally the transformers and their associated control systems, are the most vulnerable components because their failure has catastrophic effects on the ability to deliver electric power in a sustained manner. Extra high voltage (EHV) transformers are in limited supply, and while most utilities in the United States and around the world have some spare transformers available, their number is based on evaluating risks other than terrorist threats. Normally, only one, or possibly two, transformers would be kept on site.

The current philosophy of spares assumes that there might be a catastrophic loss of a transformer for a specific reason—an internal flaw, overheating, or a local natural disaster. If a transformer were lost, the installation of an available spare would cover the contingency. A well-planned terrorist attack would not occur at a single point, impacting a single transformer; rather it would be a multipoint attack. If we consider scenarios for multipoint attacks where each terrorist group involved had a high-powered rifle, rocket-propelled grenade, or a truck loaded with high explosives, then a significant number of transformers could be destroyed simultaneously. If such attacks were to occur in a country with a highly developed power grid, the power delivery capability of that country could be limited for months, if not years, because of a lack of spare transformers.

In addition to scenarios for physical attacks like those described above, we must also consider a potential cyberattack on the electric power system. A cyberattack on these systems would be similar to the general cyberattack that Seymour Goodman discussed earlier. Existing monitoring and control systems have some protection against generalized hacking, but terrorism scenarios are not contemplated in their design. It may be more appropriate to use something like a virtual private network (VPN) to interconnect control systems and equipment for data transfer.

Generally speaking, there is an energy management or state estimator system atop the hierarchy of intelligence and control of a power grid. This state estimation and control system calculates state estimates in quasi-real time. It estimates how the grid would react to the loss of one or two of the most critical (weakest link) components in a grid. These (n-1) or (n-2) contingency estimates are adequate for most cases of equipment failure or natural causes. However, a multipoint attack on an electric utility grid would be an (n-k) contingent event, one that the grid is not capable of handling. Can science and technology help to develop an algorithm that would allow the grid to recognize that it is under a multipoint attack and take action to preserve the grid as much as possible?

Deregulation, which was a contributing factor in the blackout in the United States on August 14, 2003, would have a similar negative effect in a multipoint terrorist attack. Before deregulation there were 25,000 transactions a year between utilities in the United

[51] In that regard, it follows that the switchyard, where the power generated is transformed to a higher voltage and then enters the grid, contains the most critical and vulnerable components at a generating station.

States that were buying and selling electricity. With deregulation the number of transactions a year jumped to 2 million in only 5 years, representing an eightyfold increase in the number of interactions. Since deregulation, the state estimation algorithm is being asked to handle more numerous power transfers that cross any number of utility boundaries, with generators attempting to follow demand signals that are not based on local conditions. The electric power grid and its controls are now much more complex because of deregulation, and this directly increases the vulnerability of the grid to catastrophic loss. This was amply demonstrated on August 14, 2003, by the failure to recognize that parts of the grid were under severe stress and failing sequentially.

Energy: Hydrocarbon Fuels

The discussion on hydrocarbon fuels will focus on petroleum and natural gas. Coal is excluded because it does not have the same vulnerabilities to potential terrorist attacks as other hydrocarbon fuels. First, coal is mostly consumed in large facilities that keep extensive stockpiles on hand. Also, a significant attack on the coal transport system is difficult because it is redundant and diverse.

The same is not true for both petroleum and natural gas. These hydrocarbons have major potential vulnerabilities that run from production threats (both domestic and offshore) to extensive gathering, storage, and transportation systems. With petroleum, an extensive refining process is also involved. In addition, the distribution of both liquid and gaseous fuels requires extensive local storage and distribution systems. Thus, the logistic system for petroleum and natural gas extends for hundreds or thousands of miles and can have some components outside of a country's national borders. This results in vulnerabilities that are much greater than those for coal.

Let us look closer at some of the vulnerabilities of the petroleum infrastructure. A simultaneous attack on one or several refineries would interrupt, at least in part, the adequate flow of products to the marketplace. We know from past experience that a disruption in the flow of gasoline causes price spikes and problems with availability. In fact, this would not be a highly vulnerable situation because it is rather a complicated process to attack and destroy an entire refinery. A refinery is made up of many trains producing product, so attacks have a very low probability of success.[52]

Having said that, a number of refineries have a unique vulnerability. It deals with a potential situation similar to what happened at Bhopal. This is not true in all refineries: it is not true for the very old or the very new refineries. It is true for a class of refineries that use toxic gases in the refining process. If these gases were released as a result of an attack, a catastrophic event similar to Bhopal would result. For this class of refineries, this vulnerability represents the greatest terrorist threat from petroleum although it is now less frequently used.

Obviously, the disruption of the supply of petroleum from offshore producers would have an economic impact. While the impact would be similar to that which was experienced during the gas shortages in the 1970s and early 1980s, the net result would not be characterized as catastrophic.

Threats to natural gas and electricity infrastructures look somewhat similar. In both cases you normally have production at a fixed point, transmission over long

[52] Other experts have noted that perhaps refinery operations are indeed quite vulnerable to attack.

distances, "decompression" stations at city gates, and delivery through a distribution system. Therefore, all that was said above about electric power grids would be applicable to natural gas transmission and distribution systems. Dissimilarly, storage of natural gas is possible both on the transmission system and, locally, on the distribution system. Of course, electricity is unique in that it cannot be stored. It must be generated as it is needed. Its instantaneous nature as an energy source is, in fact, one of its vulnerabilities. For that reason, electricity is the most vulnerable of all energy infrastructures.

Civil Infrastructure: Cities

The other portion of the physical infrastructure encompasses civil systems, including cities, water and wastewater, and transportation. These areas may prove more fruitful for potential joint science and technology projects, since the United States and India have experienced attacks on buildings. While the attack on the World Trade Center was dramatic and highly visible, there have been a number of attacks on symbolic buildings in India as well. What are the lessons learned from these events? Do they offer us opportunities for collaborative efforts? The first thing that comes to mind is the way in which the response to the attack is handled.

First, communication and coordination is required. When the September 11, 2001, terrorist attacks occurred, the New York City Response Center was in the World Trade Center. So the ability of the fire and police departments within New York City to respond was hampered severely because there was no way to centralize and coordinate the actions of the first responders. The lesson to be learned is that redundant response centers are needed for just this sort of contingency. The lack of communication was another lesson coming from the World Trade Center disaster. There is a definite need to have common systems that will allow all parties to communicate seamlessly.

There are other considerations for first responders. They are asked to enter dangerous or hazardous situations, and they need to know in real time whether or not there are any toxic materials present. Whether it is asbestos, biological materials, or chemical materials, the first responder needs a real-time detection system that will alert him or her to the danger.

Regarding building structures, another lesson can be drawn from the attack on the Pentagon. The Pentagon was hit exactly at the point between a newly restored portion of the Pentagon and the old Pentagon. While there was damage to the newly restored section, there was no structural failure to that part of the building. The walls absorbed the energy of the crash. In contrast, the old Pentagon suffered severe damage. Its walls collapsed. Most of the loss of life was in the old part of the Pentagon. The lesson here is to incorporate blast-resistant designs and materials into high-profile buildings.

The September 11, 2001, experience showed us that we must revisit our assumptions of the way people should exit buildings, specifically in emergency situations. Again, there are lessons to be learned about the size and structural design of stairways, and the control of airflows within them.

Water and Wastewater

As a system, water has many of the same attributes that natural gas and electric power have, namely, a source of supply, a means of transport to urban areas and cities, local storage, and distribution. Generally speaking, the transmission portion of a water system is not as complicated as in the other two cases; however, attacks on water systems can be serious, especially in contamination of the water supply.

Water also has a flip side, namely wastewater: its collection, treatment, and disposal. The major threat here is the potential for large-scale contamination if the wastewater collection and treatment systems were rendered inoperative. This could lead to human health problems as well as to contamination of the receiving waters—rivers, lakes, and oceans.

Dams and reservoirs are special components of a water supply system. Reservoirs are multipurpose. They are used for freshwater supply, power, irrigation, and recreation. They are a very important part of our infrastructure. As such, their location is also a critical element. They may be targets of terrorism, since the failure of a dam may result in the catastrophic loss of life of people living downstream.

The interdependence of infrastructure systems was dramatically demonstrated by the August 14, 2003, blackout in the northeastern United States. Parts of the city of Cleveland, Ohio, were without a freshwater supply for 5 days because the only means of delivering water required pumping and the only power supply for the pumps was from the power grid that was completely down. Fortunately, the existence of a bottled water infrastructure meant that there was water at least for drinking purposes.

Transportation

In recent years, elements of the transportation system have become the mechanisms for terrorist attacks. On September 11, 2001, commercial airliners were used as cruise missiles. The automobile has become a favorite mechanism of terrorists in such places as India, Iraq, Israel, and Palestine. Ground transport is a favored approach for bringing terror to a local population, whether by planting explosive materials on a bus or by a suicide bomber boarding a bus or driving a vehicle into a crowded venue or building.

Terrorism by means of transportation systems is very difficult to prevent because these systems generally are open systems. While security at airports and on airplanes has been greatly strengthened, most other transportation systems, for example, roads, rail, ships, are open. The situation is compounded by the large diversity of owners of the various transportation systems. There are fixed systems such as airports, railroads, and highways that are generally owned by governmental bodies. The vehicles—airplanes, ships, trains, and trucks—that are used within the fixed systems are generally owned by private entities. Transportation is vast, it is diverse, and it is global. It is integral to the global economy.

SCIENCE AND TECHNOLOGY OPPORTUNITIES: RISK ASSESSMENT

It was mentioned earlier that there is a need to prioritize the vast number of possible terrorist scenarios. Everything cannot be done at once. How can we go about systematically ordering and making decisions about the parts of the fabric of society that should be considered first? How do we apply limited resources to a wide set of threat scenarios? To accomplish this requires that adequate tools be available to do a meaningful assessment of risk and consequences.

Quantitative risk assessment (QRA) methodology will allow decision makers to prioritize risks and vulnerabilities so that they can be dealt with in an orderly fashion. Risk assessments have been used in a variety of industries. They have been used most extensively in the commercial nuclear power industry to do low-probability, high-risk assessments of damage in nuclear plants. The chemical and transportation industries have also used QRAs to some extent.

The basic approach to QRAs involves answering three questions:

1. What can go wrong?
2. What are the consequences?
3. What is the probability that the scenarios will occur?

Thus, a QRA analysis has three parts:

1. threat assessment to analyze the initiating events of a terrorist attack
2. systems analysis to define the damage states of the system being attacked
3. vulnerability assessment

The output is translated into a structured scenario connecting the initiating events with the end states. To carry out QRAs for a wide variety of possible threats is a daunting task. It may be an area of possible cooperation between the United States and India.

SCIENCE AND TECHNOLOGY OPPORTUNITIES: NEAR TERM

Fixed Infrastructure

What are the science and technology options for strengthening the various infrastructures discussed above? For cities, one of the areas that is most in need of immediate attention is the ability to respond to catastrophic events. There is a need for simulation models, improved communications, and associated training. There is also a need to conduct systems analyses of responses to events in both space and time.

For transportation systems, there is an immediate need for intelligent “information agents” for cargo. These agents would include a combination of global positioning systems and sensors to detect intruders and, possibly, the presence of certain materials as well as shipping documents detailing the contents. Such agents would be installed on every freight car in a rail system, every container on a ship, and every container

transported by truck. Thus, one could monitor at every point in time exactly where each container or rail car is, what it contains, its destination, and whether there has been any attempt to tamper with or enter it. The various pieces of the so-called intelligent agent exist today and have been used on a limited basis. Efforts are under way to marry these various components into the type of agent I have described.

Cargo scanning technology is complementary to the intelligent agents. While cargo scanners do exist, there is a need to integrate various components into a "one-stop shop" to monitor for specific items or radioactivity. The scanning equipment should be located at the point of embarkation of the container to prevent lethal weapons from reaching their intended destination. What good would it be to identify a nuclear weapon in a container as you offload it in New York Harbor?[53]

Transportation technology needs to extend beyond the cargo. There is a compelling need to develop means of rapidly identifying people, checking them and their luggage. Although there are systems in place today, the sheer numbers of people and locations is daunting. The use of biometrics would greatly alleviate this problem, while increasing the confidence level of the security forces.

Rapidly deployable barriers to keep underground structures and tunnels from being flooded are another need. Such barriers would be deployed if an attack was imminent or had begun.

Energy Systems

Reliability standards are not mandatory and are applied unevenly in most countries. The results of the power outage in the northeastern United States on August 14, 2003, demonstrated the need to do something in this area. There is a definite need for a grid to increase its resilience at the onset of an outage. The use of QRA would be an asset.

To repel physical attacks and cyberattacks, existing physical security and cybersecurity technologies can be applied. Generally, physical barriers at facilities were installed to keep people out for their own safety. Keeping people out for safety reasons and keeping them from intruding because they want to do physical harm to equipment are two separate matters. For example, a fence surrounding a substation will not deter terrorists. They can fire a high-velocity bullet or a rocket-propelled grenade into a transformer from far away, or they can drive a truck loaded with explosives through a fence. Therefore, the hardening of critical facilities is a must.

In substations, various components can be upgraded or modernized to be able to react to sudden changes in power over transmission lines when the line is under electrical stress. New electronic, solid-state devices called FACTS (Flexible Alternative Current [AC] Transmission Systems) can be used. The various FACTS devices are based on the use of solid-state power electronic controllers and thyristors, which provide fast-acting control capability to allow[54]

- greater control of power flows (elimination of parallel path or "loop flow")

[53] To deter theft of nuclear weapons, scanning at the portals of weapons storage facilities would be optimal.
[54] Hingorani, Narain. April 1993. *IEEE Spectrum.* Vol. 30, No. 4.

- loading of transmission lines closer to their thermal limits
- greater power transfer capability (thereby reducing reserve requirements)
- prevention of cascading outages (by limiting failure consequences)
- damping of power system oscillations

FACTS devices are derived from technology developed in the 1960s for high-voltage direct current applications. They have been introduced into AC systems on a limited basis over the past 10 to 15 years. The devices can range from static volt-ampere (VAR) compensators, static synchronous compensators, static synchronous series compensators, thyristor-controlled braking resistors, or series capacitors or reactors, thyristor-controlled voltage regulators, and phase-shifting transformers and unified power flow controllers. In addition to the control capabilities themselves, it should be recognized that these devices are electrical in nature and, as a consequence, can act much faster than the current state-of-the-art electro-mechanical devices (circuit breakers, switches, relays, and so forth).

One major added feature of FACTS devices is their ability to increase power flows over existing lines and measurably add to the overall reliability of power systems. It is possible that a study of the use of FACTS systems within the Indian power grid may be beneficial.

For oil and gas, there is a need to look at process technology at specific refineries to mitigate the risk of toxic gas release. Beyond that, what is mentioned for electric power applies equally to oil and gas systems.

SCIENCE AND TECHNOLOGY OPPORTUNITIES: LONG TERM

Cities and Fixed Infrastructures

One of the most important needs is for advanced sensors to aid the people put in harm's way, namely first responders. They are being asked to respond to situations in which they may not know exactly what is present. The vision here is a sensor that would be located on their body that could indicate that they have a particular chemical or biological agent in their environment and that they need to take certain precautions. If we do not do this, it makes it a lot more difficult to ask first responders to go into burning buildings or to other locations.

This same class of sensors would be useful in the heating and ventilating systems of hotels, large office buildings, and banks. Since the air in large buildings tends to travel some distance from the intake and fan system, one could include intelligence with the sensor that would cause action to be taken. For example, if some danger were detected, the damper would close before the air is delivered to habitable spaces, similar to what is done in nuclear plants today.

For transportation, the main focus has to be on a systems approach to the development and rollout of a coherent layered transportation security system. Many of the parts of this system were discussed above. It will involve advanced sensors and biometrics as well as intelligent agents. With the development and marrying of technologies, more sophistication will be possible. For example, the intelligent agent for

a truck cargo container may include a "permissive" that allows only a select number of people to drive a particular truck and requires that an eye scan be done for confirmation. There are many ways to bring together technology to minimize potential terrorist threats.

Energy

The most important technological need is for an intelligent, adaptive power grid. We need to develop a state estimation program that can sense in real time that the grid is undergoing simultaneous attacks to selected key components. As a result, it would automatically adopt an islanding scheme to keep as much of the system up as possible. This would mitigate the effects of an attack. The modernization of the grid is required to accomplish this.

Today the grid is a mélange of equipment, some of which dates back nearly 100 years. In one sense the electric power system in just about any country is at the same point that telephone switching was at 40 years ago in transitioning from electromechanical systems to solid-state electronic systems. The transformation of electric power grids from clumsy, slow-acting, electromechanical devices to electronic ones will make the adaptive grid a reality.

One last electric power technology worth mentioning is the modular EHV transformer. Historically, utilities have just a few spare transformers in stock in the event of an outage. Obviously, the planning for spares has not considered the potential need for a large number of transformers at the same time. Given that fact, and the long lead time for the manufacture of new transformers, the concept of a modular, portable, universal EHV transformer makes sense. It would not be the most efficient, most economical unit, but several of these transformers could be held at utility or regional locations to be used in emergencies and if terrorist attacks occur. Their sizing should be dictated by the ability to move them quickly and conventionally by truck to the places where they are needed.

Data Mining and Evaluation

Technology exists, and all parties want to use it to their advantage. This includes terrorists. Terrorists are going to become more intelligent and use technology for their benefit; thus, it behooves us to use technology to our advantage and to always keep at least one step ahead of the opposition.

MAJOR THEMES

One of the stated goals of this symposium was to select items for potential collaboration. The major themes addressed in this paper are listed in Box 11-1. The interdependency of the various infrastructures cannot be overlooked. Serious thought needs to be given to this subject and to approaches to mitigate the effects of terrorist threats to major urban infrastructure systems.

Box 11-1
Major Themes

Interdependency of Infrastructures
Quantitative Risk Assessment
C3: Command, Control, and Communications
Planning, Modeling, Simulation, and Training
Sensors, Intelligent Agents
Surveillance
Materials

QRA is a logical first step to facilitate the prioritization of science and technology needs. C3, planning, modeling, simulation, and training are needed for first responders as well as for the major players in each of the infrastructures. Sensors and intelligent agents are more important for transportation, fixed infrastructure (buildings), and first responders, but their applicability is fundamental to improving security. Finally, surveillance and materials are needed quite broadly.

There are several recommendations for collaboration that are worthy of further discussion between India and the United States. First, QRA is valuable in helping to set science and technology priorities. Second, given the scientific talent that exists in both countries, bilateral efforts would also be worthwhile on the topic of biometric identification technologies. Studies on the use of FACTS-based technology for power grids would also be worthwhile. Finally, a review of blast- and fire-resistant materials and the design of safer buildings (egress in emergencies, ventilation systems, and so forth) are excellent topics for discussion.

12

Discussion of Terrorist Threats to Urban Infrastructure and Relevant Science and Technology Responses

M.K. Narayanan and Richard Garwin,
Discussion Moderators

M.K. Narayanan, discussion moderator, stated that in his experience science and technology help in efforts to strengthen key aspects of urban infrastructure, but there was still a problem of matching technology with intelligence; the latter always seemed to follow, rather than precede, a terrorist event. There is a major divide between the world of the intelligence practitioner and that of the scientist and technologist. Except for electronic intercepts, Narayanan stated that he was not sure how helpful technology had been to the intelligence community. Intercepts and phone taps and other intrusive devices have improved over the years, and India has used electronic jammers to protect very important persons. However, these uses are few and far between, and more are needed. Narayanan noted the assistance of the Defense Research and Development Organization (DRDO) in developing profiling techniques, in distinguishing between the kind of explosives used by different groups, their preferred weapons, and so forth. In all this we received a great deal of assistance, but there are areas of vulnerability. The Indian estimate is that in about one-third of the cases, airport baggage screening is inadequate, and profiling of passengers has proved to be extremely inadequate. Even detection of fake passports has proven to be inadequate.

Narayanan noted that for road protection, mentioned by Lawrence Papay, technology has not noticeably assisted in the reduction of terrorism, as is evidenced by the six or more attacks on the Banihal tunnel on the strategic Jammu-Srinagar highway. Newer threats include maritime shipping, where it is estimated that nearly 90 percent of all the transport of goods is by sea. India knows, via both human intelligence and intercepts, that terrorists are paying more and more attention to shipping lines, which have generally been outside their purview of major attacks—only the Liberation Tigers of Tamil Eelam (LTTE) have done this. As for container ships, this is another problem: when will we take steps to deal with the problem, and how many container ships are going to be blown up before that? There has to be a closer marriage between science and technology and container safety, but the biggest problem is that there is a certain

unwillingness of scientists and technologists to associate with the intelligence community, and even more so with the police community. There is also a feeling of intellectual jurisdiction: the technical missions depend on the relationship between the scientific advisor and maybe the director of the intelligence bureau, but it stops with them; beyond that, nobody is really interested.

Narayanan observed that in India there was concern about the threat from radiological dispersal devices (RDD), which may be a bigger threat than is commonly believed. India has very few emergency operations centers, and those that exist are ill-equipped to deal with an RDD. While India's nuclear installations are well protected, the tracking of radioisotopes, which can be used in a dirty bomb, in hospitals and other places is lax, partly because of the cost, and there have already been several instances of theft of radioactive materials from hospitals and other facilities.

Moving from the radiological to the biological, Narayanan observed that there was a total vacuum in understanding about probable threats. Most people do not really know what constitutes a biological weapon, and it frequently takes some time to decide whether an attack has occurred because of natural causes or a terrorist effort. Biosecurity is certainly one of the areas where Narayanan thought there was a clear case for marrying technology with the protective arms of the state, the intelligence services, and the security forces.

Narayanan observed that as for the role of the private sector in both biosecurity and radiological security, there was a very important role, but he doubted whether any of the private laboratories or research centers were fully equipped to respond properly. We need the help of science and technology, but how much of it is available within the next few weeks or the next few months? This is really the question. As for cyberterrorism, he did not believe that India was fully prepared to respond.

Richard Garwin, discussion moderator, focused on two problems: the development of the "smart" container and the vulnerability of the electrical grid.

He noted that existing technology, such as global positioning systems, bar codes, and Radio Frequency Identification (RFID) could allow for comprehensive tracking of containers around the world. Today, few containers coming into the United States are tracked at all (in the sense that the container does not have a very visible number on it). Containers have a numbered seal, and before the container is taken off the ship or sent via another mode of transportation, the seal is painstakingly read and compared with the manifest, which is sent to the United States before the container arrives. About 11 million containers a year enter U.S. ports; each of them costs on average about $1,500 to manufacture. A refrigerated container costs about $3,000, and a container is used about 50 times over its 10- or 15-year life. So the amortized cost, if you take a refrigerated container, is only about $50 to $100 per transit. The cost of transatlantic or transoceanic transport ranges from $500 to $1,500, and has fluctuated by $500 during the last few years. Nevertheless, people in the industry complain that if an additional charge of $50 per container transport were imposed, it would ruin the industry. This is nonsense, as the rates and costs fluctuate by as much as 10 times that amount per transport without any effect on the industry. Indeed, a U.S. importer, Tommy Hilfiger, uses refrigerated containers not because the shipped clothing would suffer without it but simply because

refrigerated containers receive expedited treatment, as all refrigerated containers are unloaded first. These refrigerated clothes arrive a few days ahead of time, and that is worth the extra cost.

What ought to be done? Citing former Coast Guard Commander Stephen Flynn, Garwin stated that for $300-$500, someone could make the kind of tracking unit that Lawrence Papay described. It would include a seal, a tag, and an interior sensor that would indicate if there has been any tampering or entry. Getting around these devices would require more sophistication than has so far been exhibited. With this smart container approach, shippers who have signed up to provide effective verification of the manifest at the time that the container was loaded, and subsequently tracked, would get preferred shipping. For example, they might be able to enter ports where other containers could not; their containers would be offloaded more rapidly, while other shippers' containers might be shunted for unloading and inspection at the shipping ports rather than at the ports of entry. In this way shippers should be able to reduce the costs associated with shipping even though they pay more for the container initially. If the $300 or $500 is amortized over 50 shipments it is a negligible cost, but the amortization costs must be included because the tracking devices will become technologically obsolete in a couple of years, like ordinary personal computers. Even though the container might last 10 or 15 years and might continue to do the jobs for which it was bought, it would not be kept that long.

Addressing the problem of electric grid security, Garwin agreed that India and the United States had different vulnerabilities. In India, disruption occurred frequently, and there were ways of coping with the problem. However, in the United States, so much of the excess had been trimmed from the system in the interest of profitability that the United States was very vulnerable, especially to simultaneous disruption in several places. The United States needs to return to something simpler: rather than optimum control, it needs control that is good enough. This could be achieved by converting the system into a set of islands, an island being a generating capacity, and a corresponding load system. This concept is commonly called Distributed Generation, and is being employed in some areas currently.

Because there is only a finite amount of generating capacity, there is a degree of energy in the spinning reserve in the short run (the kinetic energy of the rotors, the connected loads are also sources of energy). This is on the order of milliseconds to a fraction of a second. Beyond that, power at electronic speeds is obtained from elsewhere in the grid. In a Direct Current system, this happens automatically. In an alternative current (AC) system, it is much more complicated than that. Rather than have the system go down, it would be far preferable to cut connections and shed load instantaneously, so that whatever live-generating capacity is locally available feeds a corresponding amount of load. After that, resynchronization must occur—a complicated problem. However, a large fraction of the system will continue to operate. So either the customer's facilities must have commandable load shedding or it will have to be done with switches belonging to the utility or the transmission-distribution system, block by block or over large areas in the environment. That is something that needs to be examined if we are going to face either natural disruption or a terrorist attack.

Transformers are a choke point, Garwin observed. Transformers for power plants are very efficient because a gigawatt power plant produces $300 million worth of product

per year at a few cents per kilowatt-hour times 6,000 gigawatt-hours of electrical energy per year. One-half percent of this $300 million will be $1.5 million per year, which will amortize a $15 million transformer. Extra High Tension transformers of up to 1,000 megavolt-amperes are available; 500 megavolt-amperes are common. They are very expensive but very efficient. One three-phase transformer is more efficient than three single-phase transformers because the core is used to better effect, but it would be better to lose one single-phase transformer than to lose the generating capacity of a three-phase transformer for months or for a year or more. Thus, it is far better to replace a transformer with one that is 95 percent efficient (single-phase) instead of one that is more than 99 percent efficient (three-phase). A simple analysis, taking into account the cost of electricity, the cost of the transformer, the variation of transformer cost with efficiency (if the cost of a transformer is proportional to one over the inefficiency, so a gigavolt-ampere transformer may cost $5 million dollars at 99 percent efficiency and $10 million at 99.5 percent efficiency) then we find that the optimum efficiency is about 99 percent and that the cost of a transformer can be about $10 million in order to minimize the expenditure overall. However, it would cost one-tenth this much to replace that transformer with one that was 90 to 95 percent efficient. This will require more intensive cooling because of the loss of a lot of power in that transformer, but if they are stacked in modular fashion out of single-phase transformers, they would be a lot cheaper to stockpile for emergency use. This kind of analysis would suggest that somebody should be early into the market to start making them so that they can be stockpiled and rapidly transported, and they would be much lighter than the highly efficient transformers, easier to transport and easier to erect. We need to do this kind of analysis jointly if we take seriously the damage that can be caused by terrorists to our infrastructure.

General Paul shared his analysis of the September 11, 2001, disaster and the response of those in New York. Under the auspices of the National Institute of Advanced Studies, he spent 3 days at Ground Zero some 2 years after the event, and visited Washington, D.C. He was impressed by the way in which the Federal Emergency Management Agency, the state Emergency Management Agency, and the New York City disaster organization made decisions on how to respond to the communities needs; they had a structure there, on the ground.

Paul also suggested that innovative thinking had to take place about the evacuation of high-rise buildings, such as those found in New York City and Mumbai. People in such buildings have to know whether they should go upward (perhaps to helipads on the tops of such buildings) or downward, or to some innovative lateral evacuation system. These are areas where engineers and science and technology can be of help.

He also pointed out that the Indian response to disaster or terrorism did not seem as efficient as that of the United States, where there are standby task forces with adequate equipment, or some European countries, such as Germany, which offers disaster management service as an alternative to military service.

S. Gopal wondered about the utility of science and technology in coping with terrorism. For example, despite the fact that all required technology was in place to avert an incident such as the September 11, 2001, attacks (radar coverage, awareness of the deviation from flight paths, and so forth), the attack was not able to be averted due human failure. He asked whether technology would be able to mitigate and compensate for

human failures? Gopal was also not sure that biometric detection would be 100 percent foolproof. He felt that the possibility of harassment of innocent people needed to be avoided by fine tuning technology

As for Narayanan's concern about the theft of radio isotopes and their possible use in dirty bombs, it would seem, according to Gopal, that sensors and other techniques should be sufficient to take care of this. In India the occasional cases of the loss of radioisotopic material have been from carelessness, but regardless, even if somebody steals some radioactive isotope materials, many of these isotopes, such as Carbon 14, are not really effective for making a dirty bomb. With a little care and lots of sensors this problem can be mitigated.

Papay responded to these points by noting that more and more attention and investment is now going into technologies such as interceptors. This might not be as useful in a rural environment, but it is helpful in thwarting international terrorism. As for the use of biometrics or improving passports, they are at an early stage. As many as 35 percent of all passports have been falsified, which shows that passport technology lags behind that, for instance, of credit cards.

B. Raman developed his ideas on the difference between the Indian approach and the U.S. approach to counterterrorism. The difference stems from the impact of September 11, 2001, on the U.S. mindset. These attacks affected U.S. thinking more than the April 1995 Oklahoma City bombing and the February 1993 attack on the World Trade Center in New York City. Until September 11, 2001, Americans believed that nothing much could happen there; afterwards they began to plan on the assumption that anything could happen. The U.S. approach is to identify all areas of the infrastructure that could be vulnerable to a terrorist attack and take whatever action is required to protect them, even if there is no specific intelligence information of an impending threat from a terrorist organization to that infrastructure. The Indian approach is to identify various aspects of the infrastructure that are vulnerable, identify those that have to be protected, whether there is intelligence of an impending terrorist attack on them or not (for example, the nuclear infrastructure, transportation, civil aviation) and for the rest of the infrastructure, take protective action only if there is specific intelligence of a likely threat from a terrorist organization.

Raman cautioned that Indians needed to think more about the threats and needs to counter them in the medium and long term. Some of the things the United States is now worried about may not be relevant to India today, but they could become relevant in 5 years or so, and to avoid a nasty surprise, as the United States had on September 11, 2001, India has to learn from U.S. experience. Instead of being complacent that this kind of attack is not relevant, that it could not happen here, we should plan on the assumption that it could happen to us tomorrow. From that point, Raman observed, it is important to identify the areas where we lack science and technology capability, and take action to build them even though they are not required today. India does not have the same level of financial and technical resources as the United States. The United States was able to respond quickly after September 11, 2001, but for India it will take much longer.

Roddam Narasimha commented that these thoughts led him to two suggestions for projects where he thinks India might be able to contribute significantly. Biometrics is one, the other is data mining, fusion, and management. This is central to the operation of intelligence services. There are many Indian experts in these areas, but their link is often

stronger with foreign customers than with Indian customers and in particular with public sector customers.

Devises such as electronic interceptors and jammers are crucial. They can play an extraordinary role in fighting terrorism in India, and while electronic systems are now in use, Narasimha does not believe that they exploit the potential Indian strengths in this area. Surveillance is another area worthy of future discussion because it is an extremely important issue for counterterrorism in India. Based on some Indian strengths, particularly in subareas of intelligence, and those of the United States, such as in technology, joint projects could be very beneficial. There seem to be certain areas where India has strengths that might become more evident through joint projects.

In response to Garwin's comments about grids, islanding, load shedding, and so forth, Narasimha added that Indians have a great deal of expertise in these areas, because they are forced to live with a transmission system that is very rational, given that power transmission companies do not make a profit on the power they supply to farmers. Therefore, they are not interested in improving the reliability. The more money they put into the system, the more money they lose. So if we examine the policies of the State Energy Commission in Karnataka, we find that the policies being followed are very rational in view of what is in their interest. Therefore, they have developed all these methods of living with an unreliable system; a lack of reliability is actually profitable for them. There might be considerable U.S. interest in these Indian methods.

Paul made the very important point that although in India natural disasters are frequent—in the last few years, there has been at least one major disaster every year—India is not yet well prepared to address them. This is an area where Indian experts could learn a great deal from the U.S. system of disaster management.

Garwin observed that there were two aspects of surveillance as it pertains to the movement of people: authentication and identification. Authentication is not so difficult—there can be a picture, a retinal scan, or a fingerprint—but this raises the problem of an adequate database. Some people advocate fingerprints; others, retinal scans; others, automated photo-identification, and so forth. Yet if we utilize only a single modality, that freezes the system so that it cannot evolve. Perhaps it would be best to have two biometric indicators on a passport or identification card; fingerprints are very stable and have been reliably used for many years, but they may be replaced by retinal scans or iris scans. Authentication is the process by which the identity of a person is verified: finding the biometric, that is, a face picture or fingerprint, should determine who the person is. First, that person has to be in the database. Second, the accuracy and validity of the database have to be very much greater to identify one in a million or more. Fingerprints are good enough, but facial recognition is far from adequate now.

Garwin also commented on sensor grids for the detection of radioactive sources that could be used in a radiological dispersal device. RDDs are not necessarily bombs, because explosives are not an efficient way to distribute radioactivity unless the radioactive material is a gas. A much better way of distributing radioactivity is with an atomizer (nebulizer), and this is also much less obvious. Most of the sources that are available in industry and medicine are gamma ray sources, which are difficult to shield, especially expeditiously. The U.S. Department of Energy has revealed that at the end of 2003 it deployed large teams from national laboratories with search sensors, some of them in grids, and they found one radioactive source as a result. It turned out that a

homeless man had found a stainless-steel source 4 years before and kept it with the rest of his worldly goods in a lockup self-storage system where he slept during the day, with his source under his pillow. This was a radium source for the treatment of uterine cancer, that was probably designed to produce about 50 Rem/hr1 at a distance of about 3 centimeters, hence about 1.2 Rem/hr at 20 centimeters.[55] It is much more difficult to find some sources that would be particularly suitable for radiological dispersal devices, that is, alpha emitters, that are not detectable from a distance and could be more easily shielded, but they are far less widely used. It is a good idea to share experience in this area as well.

S. Rajagopal raised the question of environmental sampling and moving detectors. In response, Garwin noted that these were explored several years ago, and a grid of sensors, or having them placed on buses (for early deployment), made sense. However, the market for sensors is very small and they cost about $1,000 each, but the price could be significantly reduced if they were made in China, Singapore, or India.

Narayanan clarified his position. While science and technology played a role in counterterrorism, especially in electronic intercepts, we do not know what is available unless scientists offer their expertise. Narayanan stated that this ought to be a major theme of the workshop: scientists should explain what they have and for what use, and this will encourage greater deployment of science and technology to counterterrorism.

[55] Rem (röntgen equivalent, man) is defined as a measure of dose deposited in body tissue, averaged over the body. One Rem is approximately the dose from any radiation corresponding to exposure to one röntgen of gamma radiation.

13

India and Agricultural Bioterrorism

Kalyan Bannerjee

All war in modern times contains elements of terrorism. In ancient times the dictum of war was the threat that "my god is better than your god, accept it or else!" In modern times it is "my system is better than your system, accept it or else!" Many authorities have tried to define terrorism in different ways but none totally satisfactorily. The whole world is now aware of the September 11, 2001, attack in New York City and suicide bombers in Israel. The western media has defined the term terrorism in a specific way. My view is that terror is a feeling, which cannot be defined. We can only give examples. What we saw on the faces of little children injured by napalm bombs, running on a village street in Vietnam, is terror, and the system perpetrating it is terrorism.[56] In modern times, war means causing maximum damage to the adversary by whatever means is possible, be it psychological damage; human casualties; death; damage to crops, food, health, properties, land, water, air; or even the annihilation of a civilization. Weapons capable of inflicting an ever-increasing amount of damage on the adversary—either immediately or over several decades—are the hallmarks of modern warfare.

Terrorism, therefore, is an integral paradigm of modern warfare. It is used by both adversaries, both strong and weak, against each other. It is in this context that this paper discusses the possibility of terrorist attacks targeting agriculture in India.

INDIA'S SUSCEPTIBILITY TO AGRICULTURAL BIOTERRORISM

The population of India has surpassed 1 billion people and it is still increasing. The country has to grow sufficient food for all of its people. At the same time, the

[56] In the Indian system of thinking, war comprises Veer Rasa (heroic mood) and Roudra Rasa (anger and destructive mood), while terrorism consists of Bibhatsa Rasa and Bhayanaka Rasa (terrifying mood). The former being the dominant Rasa in cases of war and the latter in terrorism. The Bibhatsa Rasa evokes a feeling of disgust and revulsion because of a gruesome or despicable act. In Mahabharata, the great hero Arjuna is described as being "Bibhatsu," which means that he never engaged in any gruesome or unfair act. Bibhatsu is an epithet for a truly noble warrior. However, we do not live in the times of Arjuna.

amount of land devoted to agricultural purposes is shrinking, and it is unlikely that more land will be brought under the plough. Further, conversion of forests or wetlands into agricultural use is beset with ecological problems such as deforestation and land erosion.

Traditionally, India has been an agriculture-based country. The "green revolution" —the introduction of high-yielding varieties of wheat and rice together with irrigation—has raised the value of agriculture further in the overall economy of the country.

In India, agriculture has never been solely a means of profit. For a very large portion of the population, it has been, and still remains, a livelihood and a way of life. Even today more than half of the Indian population depends on agriculture and agriculture-related activities for their livelihood. The concept of a farm as a factory is alien to the Indian population. Tradition and the small size of landholdings make Indian agriculture heavily dependent upon cattle. Indian agriculture is based upon cattle- and buffalo-drawn power. The number of cattle needed for milk production is also large. Animals transport agricultural products in the villages. During the last 20 years, milk production has been enhanced. This was achieved by crossing high-milk breeds with local breeds. These animals are of great economic value in the rural sector of the country.

India's citizens generally refrain from eating beef on religious grounds. Beef production in India is not a very important economic activity. However, there is a large, but clandestine, trade of cattle between India and her neighbors Bangladesh and Pakistan, where the animals are slaughtered and consumed. It is not known whether these countries export the meat from these animals.

The total economic value of this clandestine trade in cattle is difficult to assess. A great danger of the illegal trade is that diseased animals will be smuggled from one country to another, leading to massive epizootics. There are many examples of the transnational and transcontinental spread of epizootics. The best documented examples are African horse sickness in India and Rift Valley fever in Egypt and Saudi Arabia. These viruses are of sub-Saharan origin. For a long time they were only found in the southern Sahara. Somehow the African horse sickness virus crossed the Sahara and reached India via Syria, Iraq, Iran, Afghanistan, and Pakistan. It caused the death of 2 million equines in India (including many equines in the Indian Army). The Rift Valley fever virus crossed the Sahara and reached Egypt via smuggled camels. It produced an immense epidemic and epizootic in Egypt. The Israeli government used very stringent methods to stop the progress of the virus to Asia. However, recently the virus has crossed through the Horn of Africa in Somalia and has reached Saudi Arabia. It is only a question of time until it reaches India.

Processing of hides in India is an important industry. Workers who process hides are susceptible to diseases carried by cattle, such as anthrax, cowpox, and buffalo pox. Meat from sheep, goats, and chickens is the main source of animal protein for a large part of the meat-consuming population in India. The per capita consumption of meat is low in India compared with other countries. Indian consumption of eggs and poultry is showing a slow and steady increase. However, the total volume of trade and the economic value of sheep, goats, and poultry in the country are considerable, as is the number of jobs tied to these industries.

The breeding and trade of sheep and goats are still in the hands of traditional

shepherds, who have a nomadic lifestyle, moving with their herds from place to place. Local breeding and sale of sheep and goats also occur, although the magnitude of these activities is difficult to assess.

Poultry farming is carried out by a few large and many small producers throughout the country. The poultry industry was the last agricultural industry to be established in India and is better organized than the others.

The breeding of animals employed for agriculture in India is entirely in the hands of small farmers or individuals. It is true that for milk animals there has been a government program in conjunction with some of the agricultural universities. A number of organized dairy farms now operate in the villages. There are a number of milk cooperatives that function as nodal points for the breeding of milk animals. However, the breeding, use, and sale or exchange of draft animals are still predominantly within the unorganized sector. The sale or exchange of animals is usually carried out at cattle or animal fairs, where the owners bring their animals for display. The fairs are held throughout the country, and people travel a considerable distance to attend these fairs. Some fairs are very large. For example, the fair at Pushkar (near Ajmer in Rajasthan) or the Harihar Chhatra at Sonepur in Bihar attracts approximately half a million animals. In addition to draft cattle, milk cattle, buffaloes, camels, elephants, and horses are also brought to these fairs. Very large numbers of animals are crowded into a relatively small place for several days. The conditions are ideal for the spread of infections among the animals at the fair and for the distribution of these infections to other parts of India.

Unlike certain Southeast Asian countries and China, wild or exotic animals are not eaten in India, except as game from a hunting expedition, which is rare. Poachers do kill some wild game. They kill tigers for their body parts and skin, elephants for their tusks, rhinos for their horn, and deer or antelopes for meat. It may be remembered that wild animals are susceptible to some of the same diseases as domestic animals. These diseases include foot-and-mouth disease, Rinderpest, and pests petit ruminants. An epizootic in domestic animals may spill over to wild animals and decimate their population. This may create problems for the preservation of biodiversity. Conversely, domesticated animals can be infected by wild animals.

During the last 40 years or so, due to sustained efforts to increase the yield of milk, there has been extensive crossbreeding between exotic (for example, Jerseys and Holsteins) and Indian breeds of cows. Exotic breeds and crossbred animals are comparatively more susceptible to different diseases than are the local Indian breeds. Similarly, in order to improve the stocks of Indian sheep, crossbreeding with Scottish and Australian breeds has been carried out. Exotic and crossbred sheep also show a greater degree of susceptibility to diseases than do the local breed of animals.

Inland fisheries and prawn culture have emerged as important economic activities along the eastern coast of India. The total value exceeds a few billion rupees. These industries are susceptible to bacterial and viral infections that cause severe damage.

Marine fishing is emerging as an important activity. It is also susceptible to certain afflictions and to poaching by fishermen from other countries.

The surveillance system for animal and crop diseases in India is rather ill developed. Diagnosis of plant and animal diseases takes a long time, and much time is lost before remedial measures can be taken. This makes Indian agriculture very susceptible to terrorist attacks.

THE IMPORTANCE OF DIAGNOSIS

A large number of zoonotic, anthroponotic, and zoo-anthroponotic pathogens cause immense damage to humankind and to animals. A number of them circulate in human and animal populations. Sometimes, they are referred to as endemic diseases. Epidemic diseases emerge when changes occur in several of the following factors:

- human intrusion in the ecosystem of a pathogen
- changes in the ecosystem attributable to man-made causes
- local and global climatic changes leading to an increase in the vector or pathogen population
- increased human and animal population pressure leading to more rapid transmission of the infecting organism
- rapid transport of humans or animals leading to the rapid spread of pathogens
- global movement of processed or unprocessed food material
- changes in vaccination policies (for example, stoppage of vaccination against smallpox has made people throughout the world susceptible to that disease)
- changes in agricultural practices
- increased storage and transport of food grains leading to an increase in the rodent population causing an increased occurrence of rodent-borne diseases
- increased urbanization and the growth of urban slums, particularly in developing countries where large urban slums constitute a new kind of ecology for the sustenance and propagation of infectious diseases
- increase in vector populations of infectious diseases leading to the rapid transmission of vector-borne diseases such as dengue and malaria
- increase in vector resistance to insecticides
- changes in the virus population that are reflected in its pathogenicity
- changes in the parasite population reflected in the increased resistance of drugs to parasitic diseases such as malaria

This list is suggestive, not exhaustive. However, it is sufficient to indicate that pathogens of humans and animals are susceptible to many factors in their pathogenicity and disease-producing propensity. An intentional introduction of a pathogen or pathogens to achieve destructive goals can be accomplished by any number of different methods or by taking advantage of the natural conditions prevailing in an ecogeographical area. Certain pathogens, such as smallpox, anthrax, Rift Valley fever, tularemia, and plague, are perpetual and can be directly employed for biowarfare. Segmented RNA viruses, such as influenza, are perpetually emerging in nature, and new variants can certainly be produced in the laboratory with relative ease. The recent synthesis of wild-type poliovirus in the laboratory, and the introduction of IL4 gene and synthetic segments of DNA in the mouse pox and vaccinia viruses respectively, to make them more virulent, point to both the triumph of molecular biology and the diabolic possibilities for inflicting harm.

When human pathogens are prepared as biowarfare agents, special precautions are required to protect the people who are making them and the people in the vicinity of the production facility. When biowarfare agents that affect agricultural crops are prepared,

precaution must be taken to contain them in the manufacturing facility so that they do not spread throughout the countryside. Nonetheless, since biowarfare agents that affect agriculture do not affect the people who are manufacturing them, they are more easily converted into weapons.

Though early diagnosis of a pathogen is essential, it is equally important to know whether the pathogen is man-made or has evolved in nature through natural processes. The rapid diagnosis of an offending organism is essential for the implementation of administrative and public health measures to prevent it from spreading. It is also key to determining appropriate modes of treatment for affected humans or animals, including the development of vaccines.

Appropriate forensic diagnosis of the pathogen can be of immense help in identifying the culprits if a bioterrorist attack occurs. There is a presumption that the courts would recognize the process and the methodology of forensic diagnosis. If a terrorist attack occurs, attempts must be made to rule out the arrival of a virus or a pathogen by natural processes and to determine its creation by artificial means in the laboratory.

It is the job of international policing and security systems to detect laboratories used for the development of pathogens. Unfortunately, the Biological Warfare Convention of the United Nations is under suspended animation. Under such circumstances, it is of utmost importance for India to develop a scientifically (and legally) acceptable system for rapid diagnosis and forensics of pathogenic agents. Recent developments in molecular biology, including genomics and proteomics, make this a real possibility. The recent work on Severe Acute Respiratory Syndrome (SARS) has demonstrated the efficacy of a microarray system in the rapid diagnosis of the virus and its recognition as a novel virus within a very short time frame. Automated sequencing of DNA or RNA viruses has also helped in the diagnosis of offending agents.

FOOD DEPRIVATION AND FAMINE

The final common path of agricultural damage is food deprivation and famine. India is considered to be self-sufficient in food grains and is a grain exporter, even though it has the largest population of malnourished children in the world. This is due to inequities in food distribution and the capacity to purchase food. India is indeed in a state of precarious balance.

The Bengal famine of 1943 (abetted by His Majesty's government) was a terrible man-made disaster. International manipulation of the food supply caused the loss of 3 million lives and had far-reaching physical and mental health consequences.[57] The Bengal famine was attributable not to a shortfall in food grain production, but rather to a lack of food-purchasing power on the part of a very large section of the population and no food distribution system to get food to the hungry masses. The famine was followed by epidemics of malaria, cholera, typhoid, dysentery, and smallpox. (In modern times, AIDS and tuberculosis epidemics add to the misery of hunger.)

It is my conviction that the partitioning of Bengal between India and Pakistan was possible only because of the consequences of the famine in 1943. The demoralized

[57] Sen, Amartya, and John Dreze. 1999. *Omnibus*, Oxford University Press, London.

population could not resist and meekly submitted to the partition plan. We should guard against this type of situation arising out of political warfare. Lessons learned from the Bengal famine should not be forgotten. In this era of globalization, the world's economic powers could conceivably manipulate the food supply of a particular nation. Possible scenarios involve giant biotechnology companies, genetically modified crops, and the globalization of agricultural products. A man-made food shortage is a real possibility.

India has 6 to 7 million tons of food reserves, but these would be wiped out by two or three successive crop failures in different parts of the country, tilting the balance from self-sufficiency to deficiency. A bioattack during a lean period could aggravate the situation beyond repair. A conventional attack on food stocks could substantially damage them. A biological attack—introduction of fungal spores or poisons—could render the good stocks unfit for human or animal consumption.

ATTACKS ON THE ANIMAL POPULATION

The sheer physical problem of disposing of carcasses would pose serious challenges such as in the case of bovine spongiform encephalopathy, or BSE, as in the recent U.K. outbreak. Needless to say, if a very large number of agricultural animals were to die, famine would be sure to follow.

The effect that a disease affecting food grains, cattle, or poultry would have on trade and commerce cannot be properly calculated. The economy of a nation can be crippled for several years by incidents such as the appearance of avian influenza affecting humans in China. The mere threat of a disease can cause extensive damage to a nation's economy. The SARS scare in China is the most recent example. Diseases in fisheries can also be very damaging. In one instance, diseases in prawns created a panic across Southeast Asia, including in India. Furthermore, diseases in domesticated animals can spill over to wild animals, such as deer or antelopes, potentially damaging biodiversity.

A number of viral, fungal, and bacterial diseases of food crops and animals are already extant within India. Therefore, it is important to determine whether an outbreak is man-made or natural.

A number of diseases affecting rice are transmitted by insects (vectors). The insect population can rise very quickly and can transmit such organisms as the Tungro virus very rapidly, causing tremendous damage to crops. In 2000, the Tungro virus, transmitted by white flees, caused enormous damage to the rice crop in West Bengal. The introduction of a vector population, which can breed rapidly or in different conditions, or can transmit the organism more efficiently, can cause much damage. Mutant strains of viral, fungal, and bacterial diseases of food crops and animals can be generated by those who seek to inflict harm. Stocks of fungal spores sufficient to infect every rice and wheat plant on earth have been produced by some groups. Rift Valley fever, Rinderpest, and new variants of foot-and-mouth disease are high on the list for ruminant diseases. Chicken diseases and recombinant viruses of influenza that can jump the species barrier (for example, from chickens to humans) are also important. New strains of natural influenza (H5Nl types in China and Hong Kong and strain H7N2 in the Netherlands) have emerged that jump the species barrier and are potentially quite dangerous.

Similar viruses can be prepared in the laboratory. Many of the viral diseases that affect animals can be genetically engineered to attack humans. The de novo preparation of wild poliovirus, of virulent mouse pox virus by the introduction of a new IL4 gene, or of a virulent vaccinia virus by the introduction of new variola virus genes are possible. They could be prepared by people with evil intentions.

OTHER METHODS

There are a number of methods that terrorists can use to inflict harm. They can burn or poison food stocks, destroy the food transport system, introduce poisons or infectious agents into processed food products or stored food grains, or pollute water with pathogenic organisms. With increasing amounts of processed food on the market, this method is likely to pose a greater danger in the future. Tampering with water quality is particularly dangerous in a time of water scarcity.

In modern warfare, the food production system of a country is often a prime target for destruction. North Koreans are not likely to forget the "object lesson in air power to all the communists in the world and especially the communists of North Korea" that was delivered in 1953, a month before the armistice in Korea and reported enthusiastically by the U.S. Air Force. U.S. bombers were dispatched to destroy irrigation dams furnishing 75 percent of the controlled rice supply for North Korea's rice production. This loss of a staple commodity slowly starved the population to death. We may wonder whether such memories are in the background as the desperate North Korean leadership plays "nuclear chicken."[58]

Historically, the Caliphate civilization in Iraq was annihilated by the hordes of Hulagu Khan (Hun), who destroyed the centuries-old irrigation system in the Tigris-Euphrates Valley. It can be argued that such massive damage to a country's irrigation system can only be done by a very powerful adversary. It must be realized that damage to a few key irrigation dams, such as those in Bhakra-Nangal or Mettur, by terrorists could cause extensive damage to India's agricultural productivity.

Who are the likely perpetrators of bioterrorism in India? At present the following groups of terrorists operate in India.

First, there are religiously stimulated terrorists abetted with foreign funds and support in Kashmir, Punjab, Bombay, Ahmedabad, and parts of the Indian state of Uttar Pradesh. Second, there are separatists groups in northeastern India, which operate solely in that region and, at present, are unlikely to get involved in grain-producing areas in other states. They might target plantations with specific diseases that affect tea. With foreign assistance, these groups may be able to extend their activities to other parts of the country. Third, there are Maoist-Marxist groups in Bihar, Madhya Pradesh, Maharashtra, Chattisgarh, and Andhra Pradesh, with possible connections in Nepal, that work predominantly in the tribal areas of these states and among landless laborers.

These groups target government organizations with conventional types of firearms and explosives. Amartya Sen and P. C. Mahalanobis have shown that during the Bengal famine, the people who were most affected were those who did not have adequate

[58] Chomsky, Noam. 2003. *Hegemony or Survival,* Henry Holt and Co., New York, p. 182.

land on which to grow their own food for the year.[59] Landless laborers, weavers, fishermen, and sailors had to earn wages in order to buy food. Many of these families were annihilated during the famine. Since the Maoist-Marxist groups rely on such people in the tribal areas for support, they are unlikely to indulge in agro-bioterrorism.

Any external power in conjunction with any one of the other three groups listed could change their objectives and modus operandi. Other domestic groups such as the Liberation Tigers of Tamil Eelam (LTTE) or global groups such as al Qaeda have not indulged in agro-bioterrorism so far. However, according to press reports, al Qaeda does have such ambitions.

WHAT CAN BE DONE: TEN PROPOSALS

As far as India is concerned, the following list constitutes a comprehensive 10-part approach to the prevention, detection, and amelioration of bioterrorism.

1. There must be an efficient surveillance system, with rapid communication systems. Public panic has to be controlled by providing appropriate and accurate information to the media.

2. Rapid diagnostics for plant and animal diseases, including fish and chickens, is important. This should include reagents for diagnosis, safe laboratories for handling pathogens, and trained employees. Modern genomic and proteomic technologies can help in rapid diagnosis and forensics. Development of a sound and foolproof system for sample collection and a transport system for sending the specimens to the diagnostic laboratory is a very important aspect of a working diagnostic system.

3. India needs to develop databases for all pathogens affecting important crops of the country. During a bioterrorist attack the perpetrators may use a single organism or multiple organisms. The organisms may be classically known pathogens, including Rinderpest, foot-and-mouth disease virus affecting cattle, brucellosis affecting milk animals and humans, and plant pathogens affecting food crops. Newly created pathogens or organisms with increased virulence or ease of transmission can be designed by people with highly sophisticated laboratories.

   For a proper diagnosis and to determine the methods of control, it is essential that the laboratory system have a comprehensive inventory of all the known pathogens with their DNA or RNA sequences in an epidemiologic-epizootic database for rapid comparison. It would be necessary to obtain the various pieces of equipment and reagent systems for rapid diagnosis and their evaluation under simulated field conditions. Development of a specimen bank for standards and a serum bank from different kinds of animals from throughout the country is a sine qua non for such an endeavor. Needless to

[59] Sen, Amartya, and John Dreze.

say, development of such a comprehensive diagnostic system requires international cooperation to technically train the personnel. Rapid-action forces for damage control must be created.

4. A sound, democratic political system that can ensure the distribution of life-sustaining food to all sectors of society during times of scarcity is the best insurance against indigenous terrorism. It must be remembered that the prolonged insurgency in Mizoram arose because the government was unable to address a near-famine situation in Mizoram caused by crop failure. Hunger produces anger: the Adivasis in central India, Andhra Pradesh, Bihar, and Jharkhand are chronically hungry, and they have turned to terrorism.

5. The legal system must be able to deter, apprehend, and punish offenders. In my opinion, the Indian Prevention of Terrorist Act (POTA) and the Indian Penal Code are hopelessly inadequate to deal with biowarfare and bioterrorism, particularly agricultural bioterrorism.

6. India must develop capabilities in i-forensics[60] for dealing with bioterrorism and biowarfare. Such forensics is totally different from ordinary forensics, and India must start from scratch in this field. India could look closely at the U.S. Bioterrorism Act of 2002 and work out a system suitable for its own circumstances.

7. An interactive system of government officials and social workers can improve food and water hygiene and detect and report anything amiss.

8. International cooperation is important for information exchange and extraditing bioterrorists. The revival of the 1972 Biological and Toxic Weapons Convention (BWC) is necessary so that a workable arrangement comparable to the Chemical Weapons Convention is available worldwide. Vectors of diseases as potential agents of biowarfare should be included in the BWC.

9. There must be continued development of disease-resistant varieties of crops such as rice, wheat, sorghum, sugarcane, pulses, and oilseed. So far, Indian scientists attempt to obtain resistant cultivars through classical genetic methods. The methodology is slow, but it has been proven to be useful. Several Indian scientists have mastered the technology, and therefore research should be continued. New molecular methods are likely to give faster results. Such methods should certainly be introduced and fostered, but not at the cost of classical methodology. Each methodology has its advantages and disadvantages.

10. Finally, we must critically assess genetically modified (GM) crops for their profitability and sustainability, and when considering "farmer's rights." GM

[60] i-forensics is the convergence of information security and criminal justice.

crops should also be critically assessed for their susceptibility to and resistance against nontarget organisms.

14

Twentieth-Century Legacy: The Challenge of Biological Threats to Twenty-First Century Bio-Medical Science and Society

Christopher J. Davis, O.B.E.

INTRODUCTION

Let me begin by stating that the phrase "Weapons of Mass Destruction" (WMD) is a misconception and in many ways quite confusing. It is said to have been a Soviet invention in the 1960s, coined for political purposes and to cause confusion. We are unfortunately saddled with it—unfortunately, because by no means can all chemical and biological weapons be classified as weapons of mass destruction. In fact, the entire purpose, especially of biological weapons, is to obtain an advantage *without* destroying anything but people (and animals of plants), however unpleasant that concept may be.

This paper offers a broad overview of the topic of bioterrorism. It attempts to cover the nature of biological weapons agents, industrial biological weapons programs, bioterrorism, bombs, and natural infections, and to offer a few examples of terrorist use of biological weapons and the kinds of lessons that can be drawn from them. It also discusses biodefense, a practical philosophy for moving forward, and the directions in which the United States is going and what some people in the United States are doing. Bioterrorism is fortunately an area where science and technology could have enormous positive impact and in which research on biodefense will also provide significant benefits for society at large in the realm of emerging and re-emerging infectious diseases for which we are currently ill-prepared.

THE NATURE OF BIOLOGICAL WEAPONS: PRACTICAL IMPLICATIONS

First, there are lethal and nonlethal agents. Plague is an example of an organism that is highly lethal. Up to 100 percent of untreated victims of the plague will die.

Plague can be compared with tularemia, which comes in two forms. Today, the more well known form is considered a debilitating, incapacitating disease. The other form is the one originally developed as a weapon. It causes substantial mortality. Thus, the approaches to these two agents are quite different, the results they produce are quite different, and the way we must deal with them will be different.

There are also transmissible and nontransmissible agents. Smallpox, which is highly transmissible, can be compared with anthrax, which is not transmissible from person to person. The significance of this is great. One individual with smallpox will infect anywhere between 10 and 50 others, creating a mushrooming problem.

There are persistent and non-persistent agents. The classic Biological Weapon (BW) organism, anthrax, is persistent and hardy. Given the right conditions, it can survive in the environment for well over 100 years. Anthrax can be compared with Venezuelan equine encephalomyelitis, a virus that is nonpersistent in the environment.

Of course, there are overarching classifications of living BW organisms, divided into bacteria and viruses. Brucella can be compared with Marburg virus, for instance, and there are many other examples. The big difference is whether or not vaccines and therapeutic treatment agents exist. On the whole, there are very few drugs available to treat viral diseases. This is a large hole in our defensive armamentarium.

There are living and nonliving agents. Plague, for example, is a living agent. Botulinum toxin and ricin, on the other hand, are clearly nonliving chemicals.

Finally, there are the even more general categories of human diseases versus animal diseases versus plant diseases. There are organisms that can attack any part of the living world that we depend upon, ranging from salmonella infections in humans, to foot-and-mouth disease in cows, and Bunt of Wheat in food crops.

So, biological weapons are a family of weapons. This must be emphasized. People talk about straightforward "ballistic" weapons, but they never confuse the use of a tank with the use of a handgun. Tanks and handguns are designed to do different jobs in the hands of different kinds of people. Similarly, it is important that the same distinction be drawn in talking about biological weapons, a family of weapons that can be used in circumstances that range from individual assassinations to mass killing of civilian populations.

THE LEGACY OF INDUSTRIAL OFFENSIVE BIOLOGICAL WEAPONS PROGRAMS

The modern era has seen several biological weapons programs, including two, in particular, that were very large. The United States had a very large offensive biological weapons program, which it unilaterally abandoned in 1969, in the lead-up to the 1972 Biological and Toxic Weapons Convention. The Soviet Union had a truly enormous offensive biological weapons program.[61] Now there are about a dozen countries that have been assessed as having, or are suspected of having, offensive biological weapons programs; without discussing details, suffice it to say that these programs and the people with the skills to run them do exist.

[61] This is one of my areas of particular expertise, as I spent 10 years in British intelligence as the senior officer responsible for global biological weapons intelligence analysis.

Some historical background may help provide an idea of the scale of these programs. The U.S. biological weapons program was completely destroyed in a very short period of time in 1969. Contrary to popular thinking perpetuated by government propaganda, it had been a very successful and extremely large program. By 1969, for instance, the part of the U.S. Navy dedicated to biological weapons trials at sea had grown to such a size that, had it been separated and given to a third country, it would have constituted the world's fifth largest navy. This is an extraordinary fact given the size of the navies of the major sea powers at the time. A great deal had been achieved in the program, which the leadership of the time decided, for a very complex set of political, intelligence, and other reasons, to abandon completely. For instance, Sergeant tactical missiles with biological warheads packed with spherical bomblets were ready for use in the field; it was later discovered that the Soviets had produced very similar designs. Essentially, these were bomblets containing a liquid agent. The bomblets were designed to be released from the warhead. They were designed either to detonate at a certain height or, in the Soviet case, to bounce and split open a few meters aboveground, dispersing their contents in an aerosol along the way.

I could speak at length about the Soviet biological weapons program and still not exhaust the data, so large was the effort. I was fortunate to be in the right place at the right time in London in late October 1989, when Dr. Vladimir Pasechnik, a very senior official from the Soviet program, became the first BW expert to defect to the West; in this case to the United Kingdom. This allowed us to start to make serious political and diplomatic progress with this issue. What we learned, in addition to what we already knew, was that the Soviet program was both very large and extremely secret. The degree of secrecy accorded it was even greater than that for the nuclear program. The reasons for this are obvious. Not only was it a strategic weapons program, it was illegal, outlawed by an international convention to which the Soviet Union was not only a signatory but also a depository power. Indeed, the Soviet Union was one of the architects of the 1972 Biological and Toxic Weapons Convention. Their program was vast in scope, with enormous amounts of research and development and the highest political backing, and under military control ultimately, although most of the work was carried out in a front organization called Biopreparat. It was really the substitute for what countries in the West and many other countries in the world built in their biotechnology and pharmaceutical industry. The result was that the Soviet Union became the world's best bioweapons developer, while their biopharmaceutical industry could not produce enough standard antibiotics to meet domestic requirements. It was an extraordinary enterprise that consumed the best and most talented medical and biological minds of a generation. It drew the most capable an inventive people into this field, and they did some incredible work over a period of 15 to 20 years.

In a bold political move involving Prime Minister Margaret Thatcher and President George H.W. Bush, taking Soviet leaders Mikhail Gorbachev and Edward Shevardnadze to task, we addressed this problem, and were partly successful, in that at least the civilian side of the Soviet program was 'dismantled.' Alas, what remains of their program, or should I say the 'core' still lies within the confines of its origins in the Russian military establishments because of inspections impasses into which we were

drawn and the failure of our political and military leadership to realize the importance of this issue at a time when nuclear instability was the greater concern. The story of how this happened must wait for another occasion.

BIOTERRORISM, BOMBS, AND NATURAL DISEASE

How does the world of bioterrorism differ from the world of terrorism that we are used to? The world of terrorism is largely one involving guns and explosive devices. How is bioterrorism similar to or different from naturally occurring infectious disease? In the biological world, what we see are delayed effects. Even the most fast-acting toxin has a small delay, and living agents have to get into the body in order to multiply. Thus, whatever we are going to observe will be observed not at the time of the event but sometime after. The assumption is that our first warning of an attack will be the occurrence of sickness in the population.

Psychology plays an important role in bioterrorism. In psychological terms, infectious diseases have an enormous impact. This is especially true in the highly developed, so-called sophisticated societies of the West that regard themselves as largely invulnerable to infectious diseases. The fact that we cannot see biological weapons agents is another psychological factor. For humans the unknown is perturbing. People can understand and come to terms with bombs and bombers because they are visible. Chemical and biological weapons, on the other hand, have an undermining effect.

Re-load, a term coined by Richard Danzig, a former Secretary of the U.S. Navy, means that the person who produced the 10 grams of anthrax involved in the letter attacks in the United States could, with relative ease, increase the amount produced to 5 kilograms. Depending on how it is disseminated, 5 kilograms of dry powdered agent could do a great deal of harm. Moreover, an agent such as anthrax can inflict harm quite quickly. With 5 kilograms a perpetrator can inflict harm on multiple occasions.

First responders involved in a biological weapons incident are likely to be different from the first responders for most other terrorism incidents. With bioterrorism it is the people on the medical frontline—doctors and nurses—who produce the response. Indeed, they may become casualties themselves as a result of becoming involved with transmissible diseases or a persistent agent.

Bioterrorism also has the potential for ***many casualties and deaths***. Terrorist attacks to date have caused relatively few casualties and deaths, but that is just an accident of history. Potentially, people could be killed in very large numbers, especially if transmissible agents such as plague or smallpox were used.

In the aftermath of a biological attack, ***diagnosis*** can be difficult and challenging, even for the most experienced physician. Everybody sees diagnosis as being straightforward, but on the whole, it is quite difficult to distinguish one agent from another on a clinical basis, particularly in the early hours of their disease development. In addition, most medical professionals are not well trained or well prepared to distinguish biowarfare diseases from other more common diseases. They may have rarely seen, or never seen, these kinds of diseases. There is also a technical aspect that is not always well appreciated. When people are exposed to ***large doses of a disease agent***, the pattern of disease may be different from that which is seen in the natural world and

may not necessarily be recognized. Additionally, the disease may progress much more quickly with much larger inoculums of a biological agent.

In bioterrorism ***the pattern*** we see is in effect an instant epidemic. There are classic patterns for the emergence of any normal epidemic or for the emergence of a period of disease in society. Biological weapons do not follow this pattern.

Obviously, the ***impact*** from an apparently small bioterrorist event can be enormous. The well-known anthrax letters incident in the United States in 2001 illustrates this.

RECENT EXAMPLES OF BIOTERRORISM: LEARNING THE HARD WAY

There are in fact relatively few recent examples of bioterrorism. If we look closely at historical record, there have been approximately 200 incidents involving toxic biological materials in the last 100 years. Most of them were minor attempts at disruption. Therefore, history is not a good indicator of the future. History does tell us, however, that it is time to take this threat more seriously.

Accounts of these incidents reveal how society at large is learning the hard way about bioterrorism. Before the 1990s, most governments paid little or no attention to the problem of biological weapons, especially in terms of defense. There is a complex explanation for this. When I first came into the CBRN[62] defense business in 1980, biological warfare was thought to be passé and defensive research and development was not accorded much priority or funding. By the time we started openly discussing the Soviet problem in the early mid-1990s, the potential impact of biological warfare had become more widely accepted, but it had produced less of an impact at the political level than you might think. It took the whole issue of the 'Amerithrax' attack to focus attention and resources on biological weapons, bioterrorism, and biodefense.

The Cases

I shall first address the Rajneeshee incident in the U.S. (Interestingly, the Rajneeshee sect moved from India to the United States in 1984. The next big incident to be examined will be the Aum Shinrikyo event in the 1990s in Japan. In 2001, of course, there was the more well-known attack with the anthrax-laden letters in the U.S.

The first case study is that of the Rajneeshees, who were trying to take over political control of the area where they lived in Oregon. They had a licensed medical facility on their commune and obtained samples of salmonella bacteria quite legitimately. They grew cultures of salmonella and spread the resulting material on salad bars in 10 restaurants in a place called The Dalles. Then they sat back and waited.

Many people suffered symptoms and became ill. There were an estimated 751 cases of salmonellosis. A few people were hospitalized, but fortunately no one died. The authorities, including the Center for Disease Control and Prevention (CDC), erroneously determined that the event was an ordinary outbreak of food poisoning, occasioned most probably by poor hygiene at one of the restaurants. They reached this conclusion even

[62] CBRN stands for Chemical, Biological, Radiological and Nuclear weapons or events (weapon use incidents), used by the U.K. security services, U.K. emergency services and the U.S. military.

though all of the signs, including the pattern of disease, indicated otherwise. In fact, there are many reasons people did not recognize this incident, and, in some ways, did not want to recognize it. However, the police later investigated other activities of the Rajneeshees, and eventually several individuals confessed to the crime. Ultimately, two people were convicted and sentenced to long prison terms for their involvement in the incident.

The next case, that of the Aum Shinrikyo sect, occurred in Japan in the early 1990s. The incident, in which about 12 people were killed and thousands were affected to a lesser extent by the sect's release of Sarin nerve agent on the Tokyo subway, is well known. However, members of the sect also undertook several unsuccessful attempts to use biological agents in the years preceding the subway incident. It was precisely because of these failures that they employed Sarin in the way they did.

The sect tried on a number of occasions to disseminate botulinum toxin by driving a car through the streets. These toxin attacks failed because of poor dissemination technique and possibly, as reported by the police, because the sect failed to produce active toxin from the Clostraidal culture they used.

In 1993, the sect failed in an attempt to disseminate liquid anthrax from the roof of a building they owned in Tokyo. Many people had complained to the police about the terrible smell coming from the building. The police could not do much about that and did not want to interfere. The anthrax they used was eventually identified as a non-virulent animal vaccine strain; a Sterne variant. Had they used a fully virulent strain of anthrax, the result, despite their poor dissemination technique, might have been a lot different. Fortunately, as it was, no one became ill.

In 1995, there was a sabotaged attempt to disseminate botulinum toxin in the Tokyo subway. The Aum Shinrikyo sect plotted to place cylinders of the material under the subway escalators. The person who was given the job, however, could not go through with it and filled the cylinders with water. As a result, the attack was foiled by one of the sect's own members in a fit of conscience.

The third example of a biological weapons attack is the anthrax letter incidents in the United States. Five letters were sent through the mail to high-profile individuals. A highly virulent strain of anthrax called Ames was used; the strain was misnamed, by the way, because it does not actually come from Ames, Iowa. In all, an estimated 10 grams of spores were used. The first person to die was an Englishman who had become a U.S. citizen many years before. He received a lethal dose of spores by merely opening a letter. Since then there has been considerable debate as to the exact quality of the agent preparation and the extent to which its aerosol characteristics changed during the course of the attacks. Suffice it to say that, since much of the crucial evidence remains *sub judice*, the perpetrators of this incident produced dry particulate agent with good enough aerosol characteristics to cause illness and death despite the poor dissemination method. The overall effect was widespread contamination of the environment wherever the agent was released or leaked from the letters. The implication of this was that if the perpetrators could produce a few grams and have this result, then it would not be difficult for them to produce 1 kilogram or even 10 kilograms or more, the dissemination of which would result in concomitantly dire consequences.

When I was asked about identifying and finding the perpetrators, I replied with a great deal of caution, explaining that the intelligence community had always worried

about attribution of such an incident or even of a large state-inspired attack. Identifying the perpetrators of any biological weapons use, if they do not confess, could be much more difficult than anticipated, and maybe even impossible, as it was proved to be with the anthrax letters.

The ***economics*** of decontamination is important. There are two figures that are relevant. After the anthrax letter incidents, decontamination of the postal sorting office and the U.S. Senate office building alone cost an estimated $72 million, and this may be a conservative figure. This is a huge sum for just these two facilities. Decontamination took a large amount of time, effort, and material. The CDC itself committed significant resources, but even then the whole exercise got off to a confused and difficult start. At the height of the anthrax letters crisis, 2,000 of the CDC's 8,500 staff were working full-time on the problem and most of the remaining personnel did some part-time work as well. All of this effort went into ameliorating the effects one very small incident, an outbreak of anthrax involving just 22 people of whom "only" five died. As yet, the person or persons responsible for the incidents remains unidentified by the authorities, although some commentators say that the perpetrator is known, but the evidence will not stand up in court.

Lessons Learned

What lessons should we learn from all this? When I was a young physician-in-training, we were told that "common things commonly occur." In other words, before looking for some esoteric diagnosis, review the common causes of pathology. On the whole, this approach serves routine medicine well. Indeed, it has become the predominant pattern of thought in everyday life. It was responsible, in part, for the reaction to the Rajneeshee incident. After all, who would have thought of bioterrorism as the cause of the salmonellosis in an obscure location in the North West of the U.S.? And when they did, just how plausible would it have seemed at the time? Unfortunately, this higher degree of awareness is required if we are to operate effectively against bioterrorism threats and attacks. In medical diagnostics this is referred to as a 'high index of suspicion.' Without it, hoof beats will always signify horses and the zebra will be upon us before we can react. If we value our survival, we simply cannot afford for this to happen.

Technique is extremely important in matters of weapons and their use. Without technique you can easily fail at simple things, as happened in the Aum Shinrikyo incident. The members of the sect could have achieved their aims, but they made some silly mistakes. Luckily for the Japanese people, they did not have quite the right knowledge and the essential technique to launch a successful bioweapons attack.

Conversely, a simple idea well executed can be very effective. The Rajneeshees carried out a primitive form of attack, using a simple dissemination system, and caused significant illness in hundreds of individuals. Be it bugs or bombs, nothing in life is guaranteed; sometimes they work and sometimes they fail. Ill-informed commentators are inclined to say, "Oh, the Aum Shinrikyo sect with all their money and scientists failed, so it just goes to show how difficult it is to use bioweapons," or alternatively that "bioweapons must be ineffective or useless as weapons and are not therefore a problem." Alas, this is the wrong conclusion to draw from these incidents.

Having lived in the U.K. through 30 years of 'classical' terrorism — something with which our Indian colleagues are very familiar — when the Provisional Irish Republican Army used a variety of devices on a regular basis, we learned that bombs did not always detonate properly. Sometimes they killed their perpetrators. The same is true with biological weapons. Even cruise missiles and other sophisticated weapons are not 100 percent reliable. It is unwise to tempt fate by judging our chances of survival by the failure rate of the weapon or the operator.

When bioweapons work, as the anthrax letters did, whole societies change their behavior. That is exactly what we have observed in the United States. Sometimes a society "gets lucky." Five people paid the ultimate price to wake us up to a whole series of problems and to prompt us to start to address them.

USING SCIENCE AND TECHNOLOGY TO COUNTER BIOTERRORISM: DEFENSE IN BREADTH AND DEPTH

From the historical perspective, bioterrorism is a low-probability, high-impact event. A little bioterror can have a big effect. That is the view we must take about how to deal with it and how much money and other resources to invest in defensive measures. The use of just 10 grams of anthrax has caused enormous changes. In the aftermath of the anthrax letters incidents, large amounts of money were spent and attitudes of the U.S. public changed completely.

In events involving infectious diseases, ***preparation and prevention*** are key to managing outbreaks. If such events catch a society unprepared, even more time and money will be spent, and even more lives will be lost than if it had been thought through in advance.

We do not understand a lot about what we thought we understood. There are many accepted dogmas about biological agents themselves, their effects, about the organisms and their physiology, pathology and effects: for many years people have taken them for granted. On the whole, these areas of science have been much neglected during the last 30 or 40 years. Scientists considered them to be boring and unproductive, and opted to do what they perceived as more exciting experimental work. After all, who wanted to look at the metabolism of some obscure bug that was no longer of importance to us when it was a simple matter to treat the problem with an antibiotic? Scientists want to do work that will build an interesting and productive career, and allow them to write papers, receive large grants, be at the cutting edge of research, and be respected by their peers. A few scientists continued to study infectious diseases, but it was not very popular. Society has suffered as a result, because there is much that is not understood, even about common diseases. Fortunately, and not a moment too soon, this parlous state of affairs is changing fast.

What we need is biological defense in breadth and depth, and I will outline the kind of actions that must be undertaken in order to achieve this. It is important to put in place widely dispersed local (point) and stand-off bioaerosol detection in order to be able to monitor the atmosphere continually and detect aerosols of biological agents. It is a very tough technical challenge. In the United States, point detection is being attempted at 36 sites across the country, but it is far from a perfect system. It is possible to develop

stand-off detection—a sort of biological radar—but this is even more difficult to goal to achieve. It may be possible in the future, but right now. More practical in the short term is infectious disease tracking in real time. In other words, systems of detection and information exchange need to pick up changes in behavior in real time.

Stockpiles of prophylactic and therapeutic agents, and doing research and development on new vaccines and therapeutics are also needed. Decisions about the tactics and the strategies to counter a wide range of organisms must be made, which is by no means as simple as it first appears. There is no multivalent vaccine that will cover everyone against everything with one shot and with no side effects. Since we lack such a vaccine, we need to be able to respond with therapeutic agents. In any case, even with effective, safe vaccines, we would probably not be able to vaccinate everyone throughout their life. Lifetime vaccination would probably be unacceptable to society at large, because the likelihood of an attack is considered to be quite small. Therefore, therapeutic agents are at least one avenue we should consider since they allow us to adapt to differing circumstances and may be used prophylactically or in response to obvious infection.

We also need real-time diagnostics for infectious diseases. Doctors, nurses, and other medical professionals need tools that can be used when something unusual is occurring, but they do not know what it is. For example, if an odd cluster of people exhibit similar symptoms—temperature, aches and pains, cough, and so forth—medical professionals need to distinguish the cause of this pattern from the common cause of such a pattern. Some science and technology should focus on this area.

There must be a robust public health system. It is well recognized that, even in the United States, this is a neglected area. Public health professionals are poorly paid and receive few thanks for their efforts. Public health care systems were built to protect us from infectious diseases in an era when people feared infectious diseases. Today, people do not fear infectious diseases, unless a resistant organism affects them or a relative, or if AIDS is an issue. In such instances, attitudes begin to change. We need trained and knowledgeable medical and nursing staff and paramedical first responders. These are the people on the frontlines, and they do not know as much as they need to about infectious diseases and biological threats.

Finally, I have to emphasize the importance of planning and of thinking the unthinkable. It was very difficult to persuade people to do this before 2001. In the end, planning is the best chance that we have to save ourselves from potential catastrophe. Political awareness and public participation are fundamental motivations for planning. Ultimately, it is the citizens who pay the bills and decide how our taxes should be spent.

ASSESSING NATIONAL CAPABILITIES

Richard Danzig, former Secretary of the U.S. Navy, was asked to write a monograph assessing national capabilities for addressing bioterrorism. He looked at the problems and suggested some approaches and solutions, proposing a list of key topics by which to judge preparedness. Danzig asked two key questions: how can we assess how we are doing, and what is our scorecard? For example, when assessing our response to anthrax, how well prepared are we today? To cope with anthrax, smallpox, or other infectious diseases, he suggested a useful list of categories to use to evaluate our

progress. This list includes detection, drugs, vaccines, decontamination, interdiction, intelligence, surveillance and diagnosis, simulation, modeling, gaming, alleviation, counterproliferation, civilian preparation, and consequence management. This list is a practical tool to use to assess what needs to be addressed.

National Preparedness: The U.S. Approach

In 2003, John H. Marburger, senior science advisor to the President, stated that the anthrax incidents sent two unambiguous messages: our society is vulnerable to bioterrorism, and we are not prepared. He said that in the intervening 2 years since the anthrax incidents, however, important steps had been taken to protect and prepare the nation for a broader range of threats. A substantial framework has been created, clear directions have been established, and very basic things have changed.

In former years, the CDC was not very involved or interested in addressing biological threats. It now has a new director and is much more involved and much more focused on the business of emerging diseases and the potential of bioterrorism and biological weapons.

Similarly, the National Institutes of Health (NIH) have never had large amounts of money to do research in this area. In recent years, however, the U.S. Congress has appropriated a lot of money to NIH to act as the agent for driving forward biodefense and biomedical basic research and development. The NIH has a very big job assigned to it and the new mission will present quite a challenge to its prevailing culture.

Funding is of course a crucial element. Very large figures are involved. Nearly $1 billion was appropriated for research and development on science and technology in 2004, with a large increase in funding going to the NIH for research during the coming years. It is quite difficult for the NIH to absorb this amount of money and to build new programs. It is all very well having the money, but it is a challenge to spend it sensibly and effectively.

Overall, the response to bioterrorism has been organized into three broad interagency initiatives: (1) Project BioWatch, or early warning using atmospheric monitoring—36 sites are now being used in this experimental project; (2) Project BioSense, or biomedical data collection and fusion to detect pattern anomalies in human disease occurrence; (3) Project BioShield, which places more emphasis in the public health domain and covers the accelerated research, development, and procurement of medical countermeasures.

Unintended Consequences

A few things can happen to a society when it is threatened, as was the United States with biodefense, and U.S. reactions have caused some unpleasant things to occur. Consider, for instance, the issue of biosecurity, where measures, including registration, have been put in place to increase physical control and accountability over highly pathogenic microorganisms. This has caused great difficulty for many scientists in the U.S. who work with these organisms, and has become a challenge to the way scientific

pursuits have always been conducted. Scientists who once worked with microorganisms under little scrutiny, now face Draconian penalties if they make mistakes with paperwork or physical accounting procedures.

This also affects international cooperation. The United States and the United Kingdom have a history of close collaboration in this area. In both countries, even within government circles where the network of people doing research and development on "Select Agents" is small and very tight, shared projects have come under pressure because of these new rules. No one has yet solved this problem as we continue to crack a walnut. We must be very careful about how we implement protective rules without knowing the ramifications of our actions.

The question of the dual-use dilemma on misuse of technology for destructive purposes was addressed by the National Academies' Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology.[63] How do we, as scientists and technologists, police ourselves against the kind of science that we think may be dangerous to our society? Can we indeed do this? When science poses danger to society, should it be confined to special sites, should the results be vetted before publication or should we abandon it altogether? These questions are very sensitive and are under debate.

THE WIDER WORLD

Out there is a big wide world in which some bad things are happening. The question of new and reemerging infectious diseases is now recognized as a rising global issue as well as a security threat. Infectious disease accounts for 25 percent of the deaths that occur annually worldwide. Since 1973, 20 well-known diseases have reemerged or spread geographically. More than 30 *new* diseases have been identified since that time. Tuberculosis (TB), malaria, and HIV/AIDS continue to surge. TB is likely to become the largest cause of death in the developing world by 2020.

In the United States, the price of public complacency about infectious disease is high. Annual infectious disease rates have doubled to more than 170,000 per year since 1980, and these figures are 3 years out of date. Four million Americans are Hepatitis C carriers, Influenza kills 30,000 Americans annually, and foodborne illnesses are in the millions, with 9,000 deaths per annum. Even in the U.S. TB has made a comeback and is still increasing. Highly virulent and antimicrobial-resistant pathogens are major sources of hospital-acquired infections, killing 14,000 patients annually. Interestingly, however, it took just five anthrax deaths to change behavior towards infectious disease in the United States.

A SILVER LINING

Despite these challenges, let me end on a note of optimism. One high profile incident of bioterrorism caused five deaths, drove U.S. society and its leaders to re-

[63] National Research Council. 2004. *Biotechnology Research in an Age of Terrorism,* National Academy Press, Washington, D.C.

examine the issues and focus on the problem of biowarfare and the related, but larger everyday problem of infectious disease. The complacency that is largely born of the era of antibiotics is slowly being rolled back. Already this new awareness has produced a better response to new challenges, such as Severe Acute Repertory Syndrome (SARS). Unquestionably, the CDC reacted in a much more publicly acceptable, professional, and speedy way in response to SARS when it was informed of the outbreak by the World Health Organization (WHO). The WHO, in turn, had picked up from its network what had happened when an infected Chinese gentleman moved into Vietnam with the disease. Clearly, the situation is improving, and people are less complacent.

PAYING THE INSURANCE PREMIUMS

Ultimately, these efforts are going to cost a lot of money, but I think this kind of expenditure is best viewed as paying insurance premiums. So, why pay insurance premiums? I believe in a defense strongly constructed in breadth and depth and openly declared. I applaud the way that the United States deals with biodefense in this respect. Its approach stands in contrast to the more secretive approach of the United Kingdom. There the view favors keeping plans secret, to be revealed only when necessary in response to an event. Actually I do not want the day of the event to come. I do not want the perpetrator to challenge my defenses. Rather, I believe it is better to show potential perpetrators what they are up against and use this as a deterrent.

Regarding bioweapons, we have no means of retaliation, and possibly no means of attribution. We have not even found the person or persons who sent the anthrax letters. We would not have caught the Rajneeshees had there not been a confession, and had the Aum Shinrikyo not been so inept, we would not have found them either. Defense is the only answer for us, especially since we are not in the business of biological retaliation. If there is a deliberate attack, of course, defense pays enormous dividends. It will ameliorate effects and minimize long-term damage. The defense systems that are proposed at the moment will not give us 100 percent protection, but then again no defensive system is 100 percent effective.

Unlike most other costly defensive or weapons programs, preparedness for bioterrorism will pay dividends everyday because it increases our ability to combat the growing hazards of "ordinary" infectious disease. Therefore, if we can deal with the very unpleasant and highly unlikely problem of weapons, at the same time we will help the people who have real, everyday needs for dealing with infectious diseases. By spending the money in one place, it will flow across to help in several other areas.

This is an area where science and technology will almost certainly prove decisive; in increasing the capability of society to ameliorate the effect of an attack or even to prevent such an attack from taking place by raising the bar of defense so high that adversaries look for more vulnerable targets. Because of the wealth of intellectual capability that India has to offer in the fields of biotechnology, engineering, and information science, prospects are good for creating fruitful partnerships between the United States and India in this sphere of endeavor.

I am not the world's greatest optimist, but on this occasion, I think that *together* we have a chance to make a difference where it counts.

15

Discussion of Biology and Agriculture Terrorist Threats

S. Gopal and Jonathan Pollack,
Discussion Moderators

S. Gopal, a discussion moderator, asked why terrorists should resort to bioterrorism against humans, animals, and plants. First, the advantage of bioterrorism is its cost-effectiveness compared with other forms of weapons of mass destruction (WMD). In one study the cost per casualty was assessed to be $2,800 for atomic weapons and $600 for conventional and chemical weapons, whereas the same study assessed the cost per casualty of using biological toxins and bioterrorism to be about $1. Another study says that, when delivered properly, the quantity of butolinum toxin needed to kill 10 people is as small as a dot of an "i". If this is so, obviously there is a tremendous advantage to bioterrorism, which is sometimes called the poor man's atomic bomb. Second, bioterrorist weapons are easy to produce. Again, according to one study, a biological arsenal could perhaps be built with $10,000 worth of equipment in a 15′ x 15′ room with gear no more sophisticated than a fermenter and a protein-based culture, and to protect the producer, a gas mask.

How effective will bioterrorism be? We must distinguish between the use of this weapon in developed countries and in developing countries.

Bioterrorism can be used against humans, and it can be spread through air or water or introduced in the food supply from the farm to the table. It can be used against livestock and animals, essentially to break the economy and create scarcity, and consequently demoralization and panic in the society. Third, agricultural pathogens can be introduced to decrease crop production, including cash crop production, and to disrupt the economy.

Terrorists using these methods need not be Islamic fundamentalists; they could be political or religious terrorists fighting against the state. Business competitors have used terrorism to ruin the business of their rivals. Cult groups, such as the Rajneeshee, could use it for revenge against individuals, companies, or the state. In the United States there have been one or two such cases. In 2003, a supermarket worker was caught introducing insecticides containing nicotine into beef.

All this is terrorism, though we tend to think that terrorism is practiced by people

of certain ethnicities or religions. It could even be state sponsored against another state, to hurt another state's economy or agriculture. Apart from decreasing food production, there is also the enormous economic cost of the recovery process, recycling food, and cleaning up the contamination. In bioterrorism against humans, one of the most feared events would be the return of smallpox. Though the World Health Organization (WHO) has declared the world free of smallpox, there are still lingering suspicions that strains of smallpox are being held for experiments. As long as something exists, there is always the chance of it showing up in the population.

Of course, there has been a lot of publicity about the danger of anthrax. Anthrax does not spread from individual to individual, and in fact, in India, anthrax exists. We have been dealing with it and there has been no panic. There are many areas where farmers know exactly where the cattle should not graze, because of anthrax-infested areas.

Acquiring or producing a very virulent pathogen is also much more difficult. This would involve access to biological scientists by terrorist groups. Aum Shinrikyo tried but failed to get the Ebola virus. It may be easier, however, to introduce anticrop fungal diseases and so forth. Assuming that these are all being done, what is the time frame in which the effect is seen? Is the terrorist willing to wait for the time frame, especially in the agricultural field? With a good monitoring mechanism, is it not possible to detect it early and take countermeasures?

These pests and strains do not recognize international borders. We have had a case of a virus affecting chicken coming from Israel, noticed in Pakistan, eventually ending up in southern India. In such cases, Gopal noted, he did not believe that any right-thinking state would intentionally indulge in this kind of activity because it can boomerang. With basic monitoring mechanisms and a well-established public health policy, this is a controllable problem. What has however been a dangerous trend in the past has been that commercial damage is tried by both state and nonstate terrorists. In 1979 Palestinian terrorists introduced mercury into Israeli oranges, which caused a tremendous problem, and in 1981 the Liberation Tigers of Tamil Eelam (LTTE) threatened to contaminate Sri Lankan tea with cyanide.

Gopal felt that bioterrorism and agricultural terrorism should be considered more from the perspective of economic damage than from that of individual damage or harm. The economic damage will be great regardless of the source of the attack, and it will be difficult to trace the source of the attack.

In agricultural terrorism we should be able to use even existing technologies such as satellite imagery and aerial imagery, and even proper monitoring by the concerned agricultural departments, to notice early enough that there is a problem in a particular area and react quickly.

Another form of bioterrorism, apart from using pathogens, could be to introduce noxious weeds; this has been a problem in India. Specifically, there was a parthenium problem in India, and it is still a problem in many places where the parthenium was not indigenous to the country. It was suspected to have come from imported food grains, and now it occupies acres and acres of land and is dangerous, and it is creating a lot of problems for humans. It is possible to weed it out, but at a high price.

This is not a kind of terrorism that is impossible to control if technologies are in place. For example, a good public health administration system throughout the country

with a network, which is connected not only with their own offices but also with individual veterinary doctors, veterinary hospitals, agricultural institutions, and even village cooperatives, would make it possible to know at once that a problem is developing. We could then deploy all available technologies to contain and eliminate it. At the same time we have to take notice of the degree of likeliness of an attack, because the economic costs may be very high. The technology required is networking, monitoring, and the provisioning of antibodies, which can take care of the problem if it arises.

Jonathan Pollack's response noted the danger of allowing the phrase "countering terrorism" to be a catchall for the world's ills. Both analytically and as a public policy issue the term is not useful even if there may be ways in which the expenditure of money may yield important and beneficial results. Pollack noted that the presentations spanned the problems that we see both in advanced industrial economies and in predominantly agricultural economies, as is India, even with its significant industrial advancement. Indeed, it highlights looking back to the title of the National Academies' report, which appropriately emphasized "making the nation safer"—not safe but safer. A theme for the kind of collaboration that we would want to see between India and the United States would be, ambitiously, how one makes the world safer.

Pollack agreed that the examples provided by the presenters offer fertile ground for discussion, but he warned that we are dealing both literally and figuratively with a very different species of threat, something for which we are not well organized collectively to counteract. This may require very different models of international security collaboration, as terrorism is a method of warfare, or a particular way of using violence, presumably for different kinds of effects. The difficulty, of course, is that effective countermeasures for one type of terrorism are not necessarily effective for other types, and as Christopher Davis noted, in some cases the term weapons of mass destruction (WMD) is a misnomer. Pollack suggested that it was Vannevar Bush who first used the term in a memorandum to President Dwight D. Eisenhower about 50 years ago. WMD as a term has been expropriated for a variety of purposes; we are most focused on the incredible destructive capability of nuclear weapons, rather than the challenges that were discussed in this panel, although Pollack agreed that both presentations showed ways in which biological threats could entail mayhem of incalculable scale. Even so, given the very particular character of some of these biological threats, because causality is highly problematic and the effects can be delayed, it may be very difficult to conceive of and cope with this problem, at least in the way we deal with specific incidents.

Similarly, what struck Pollack in some of the examples provided in both presentations was that the relevant examples tended to occur within societies rather than on a transnational basis. Further, Pollack asked, if some kinds of terrorist attacks are indeed so feasible, why have we not seen more of them—does this suggest that such incidents and activities have been foiled? In Pollack's view, most of what we must deal with in these realms is in the core competencies of different terrorist groups. They do very well at shooting people or blowing them up; they do not seem to have core competence in wielding weapons of mass destruction.

Pollack also pointed out that we do not live in a world of boundless resources, and we have to grapple with questions of allocating our effort to the areas where we can

achieve the most beneficial results. Pollack's final comment on Davis's presentation was that we do need to be aware that our heightened awareness about biological attacks stems from the anthrax incidents. Had they not taken place, it is doubtful whether we would have seen a renewed interest in infectious diseases in the United States and elsewhere in the developing world. He suggested that we need to seize this opportunity to expand research on such issues even if it takes us well beyond issues of terrorism.

Turning to Kalyan Banerjee's presentation, Pollack suggested that we need to know more about what the political effects of bioterrorism might be on a vulnerable, predominantly agricultural, economy such as India's. Pollack noted that most instances of famine, and the use of food as a political weapon, were politically induced within various societies, often inflicted on the populations of those societies by the people who claim to lead them. Some examples of this include the extraordinary famine in China after the Great Leap Forward (1959-1961), where perhaps as many as 30 million people died, and the North Korean famine in the mid-1990s, when perhaps as many as 1 to 2 million people (or approximately 5 to10 percent of North Korea's population) died. Other examples of state-induced famine or biological disaster are evident in Africa. So often the villain is from within; we have to remember this as we search for effective ways to deal with these looming crises.

In the subsequent discussion, Vijay Chandru touched on two points: the issue of public-private partnership cooperation in the U.S.-India context, and India's capacity to respond to threat. He pointed out that his own (Indian) biotech company has investments from Goldman Sachs and several U.S. funds, but is also supported by the Indian government through soft loans and research and development money from agencies such as the New Millennium Initiative of Council of Scientific and Industrial Research (CSIR), the Technology Development Board, and the World Bank fund through ICICI.[64] Private companies have already transcended national boundaries, and his company has U.S. board members and maintains a branch office in San Francisco.

In addressing the problem of real-time diagnostics for infectious diseases, Chandru noted that Indian technical and scientific capabilities to build such a system already exist. The idea here, of course, is that there are viral and bacterial infections and various strains of these infections and mutations, and we need to be able to diagnose very quickly. High-throughput technologies such as microarrays and polymerase chain reactions (PCRs) are certainly most appropriate for doing this. However, in designing these microarrays, since these are DNA-based technologies, informatics are heavily involved in looking at the genome sequences and selecting the right representative oligonucleotides, and so forth. The agencies in India that Chandru had interacted with, and that might be helpful, include the Institute for Genomics and Integrated Biology based in Delhi. The institute possesses the sequonome mass array system that can be used for rapid sequencing. They also do spotting of microarrays and PCR. He noted the existence of other groups, such as the Center for DNA Fingerprinting in Hyderabad, which is also a candidate for collaboration, just as there may be similar collaborative projects in the United States. Chandru suggested that it would be useful to bring these teams together.

He referred to a case study of upper respiratory viruses that Strand Genomics Ltd.

[64] The Industrial Credit and Investment Corporation of India Limited (ICICI) was incorporated at the initiative of the World Bank in 1955.

had conducted by looking at essentially the whole genomes of various viruses and viral pathogens and developing a diagnostic array that could distinguish, that is, look for specificity but also look for conservation across genera. Because of mutation problems, we want to be able to identify at least the genera from which a particular viral pathogen comes. In one case, Chandru's company has designed a virtual microarray and runs a simulator of hybridization including all the thermodynamics of hybridization in the background. It is possible to submit a sequence, and this virtual microarray will light up, indicating from which particular virus strain this may come. Chandru noted that this information is available on the company's Web site, the database is public, available from the WHO, and various groups in Singapore use the technology. These capabilities are in India and are available for cooperative projects.

Lewis Branscomb asked about the relationship between infectious pathogens and chemical toxins that might be used in terrorism, since both share a common set of features, one of which is the need for a distribution system to distribute the weapon. He added that serious thought ought to be given to the various systems in society through which either pathogens or chemicals might be distributed to a very large number of people in such a short time because it might be impossible to shut the distribution system down in time. Branscomb pointed out that this was a feature of the anthrax attack, because the letters in the mail were contaminating one another and the authorities did not know how many there were. If someone in a factory manufacturing postage stamps were able to contaminate one day's production of stamps, there would be a significant effect, especially if the stamps had to be licked. In this particular case, because stamps come from one place, it would be relatively easy to implement a set of controls and tests, but with newspaper delivery, or the distribution of bills by banks, and other examples, it would not be that simple.

K. Santhanam made four observations regarding agricultural terrorism. First, in his view, agroterrorism could amount to economic warfare and it may affect an economy, and he would treat it differently than terrorism associated with the chemical industry or agriculture. Santhanam submitted that terrorism affecting the economy of a country, and its trade and commerce, fell into another important category. For instance, prawns that were exported from India to Australia were claimed to have salmonella. Sales declined and prawn exports from India to other parts of the world, especially from Goa and Orissa, and some parts of Tamil Nadu, were affected. There might have been commercial reasons behind the scare.

As for the leakage of chemical, biological, and nuclear materials and agents out of the former Soviet Union to other places, we have been told that there are no problems. There was a CBS *60 Minutes* story describing an ampoule containing a biological agent that someone had acquired in the Pakistani city of Quetta—weaponization had occurred. Santhanam asked how we would respond to a major source of leakage and seepage, not just of agents, but potentially of technologies as well.

Santhanam's third comment referred to Project BioWatch, which was mentioned by Christopher Davis. His view was that the thief has to be halted before reaching the intended target, and therefore international cooperation of a very high order is required to keep this dangerous material from getting into the atmosphere of a small town in the United States. Regretfully, Santhanam pointed out, the trends are otherwise, and attempts to make the 1972 Biological and Toxic Weapons Convention (BWC) stronger and more

enforceable were systematically frustrated, given lower priority in U.S. diplomacy because it might have had an impact on the U.S. pharmaceutical biotech industries.

Finally, Santhanam discussed cases where a planned attack might be disguised as an act of nature. There was an early U.S. program of weather modification, which was aimed at the Cuban sugar crop. The success or failure of this kind of cloud rustling is less relevant than it being imagined; also, he noted, the scale of disturbance noted in the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques was left delightfully vague. There is also the example of foot-and-mouth disease in Taiwan, where they are convinced that this was actually exported by China to cripple Taiwan.

In his response, Davis agreed that the Taiwan case was extremely suspicious, wiping out Taiwan's entire pork industry (and they were the main pork producers for the entire region). The variant came from China and yet we still cannot prove that it was deliberately transported to Taiwan.

As for Santhanam's comment on BioWatch and the BWC, Davis suggested that while international cooperation is needed, the BioWatch system is the first ever established and is still in an early stage (it has 36 sites now). Davis explained that the BWC was connected closely with politics at the highest level, and that in his judgment there seems to be no way of getting all of the concerned parties to agree on a convention that actually makes sense and is enforceable. He knew of no one who had a good idea on how to solve the political impasse; there is a basic unwillingness of countries to allow teams from abroad to walk in and inspect their facilities.

Santhanam then suggested that if the United States felt the need for a new nuclear materials proliferation security initiative (PSI), then he was sure that it would be enlarged to chemical and biological as well, including seizure of ships on the high seas. This would certainly be outside the BWC, but what we might see is a PSI of like-minded countries, with Britain in the forefront. The radius of the circle may be enlarged, but still it will be a "little club" approach, and less effective than a larger internationally agreed approach to such problems well before they reach the U.S. mainland.

In his closing remarks, Banerjee commented on surveillance of potential agricultural or human diseases, stating that it has to be done on a global level, sharing data. Without that, he doubted that much could be achieved in the prevention of terrorism or warfare using biological weapons.

Banerjee also suggested that there ought to be a national serum bank system, where serum and blood samples taken from throughout the country may be stored and tested for the presence of a virus or disease. It would serve as a baseline to determine if detected disease was new or old.

As for Santhanam's comments on the BWC verification protocol, he noted that there had been vigorous protests against it, bringing the BWC close to a standstill. These protests are partly justified for corporate business interests, yet a lot can be done in situ without taking any material or property outside. There is no reason why in situ verification cannot be done, so that nothing leaves the system of a particular corporate organization.

Banerjee concluded by discussing the possible use of corporate groups to manipulate the agricultural production of a country. That problem has to be solved, he emphasized; it cannot be evaded by saying that this is important to free enterprise. Free

enterprise yes, but free enterprise to squeeze others is not acceptable. Banerjee summarized his view with the aphorism, "corporate business corrupts and consumer corporate business corrupts consummately."

In the final remark of this discussion on bioterrorism, Rose Gottemoeller expressed her agreement with Santhanam's concern about the PSI tending toward a club-like arrangement; she noted that there were many in the George W. Bush administration who were highly resistant to legal mechanisms of various kinds, particularly on a multilateral basis, and preferred informally articulated arrangements. In Gottemoeller's view, they have realized that the PSI needs some legal underpinnings, and they are looking at drug interdiction as one model; furthermore, there are already legal arrangements in place, in the context of the International Maritime Organization, for interdiction-related issues. Of course, she concluded, having adequate intelligence capabilities in place for interdiction is as important as developing a legal underpinning for the PSI.

16

Why Should India and the United States Cooperate?

K. Santhanam

The question, in my opinion, is not why the two countries should cooperate. Rather, it is one of whether India and the United States can afford *not* to cooperate on counterterrorism.

My response to this question is simple. It is necessary for two main reasons. First, do not ask who will be affected by terrorism; know that you will be. It is true that terrorism ultimately affects everyone, but it is especially true for open and pluralistic nations, such as India and the United States, that follow a secular and democratic system of governance and accommodate political dissent. These nations constitute a vulnerable "special community."

Second, to tackle and subdue terrorism in its allotropic modifications, there is a need to share knowledge and experience in different phases, ranging from detection to deterrence and destruction of terrorist organizations.

PARAMETERS FOR INDO-U.S. STRATEGIC COOPERATION

What parameters should be considered in an effort to establish strategic cooperation between India and the United States on counterterrorism? Do these conditions exist today?

To my mind, the first parameter is the convergence of perceptions about terrorism and terrorist organizations. This convergence need not be full or absolute, but at a minimum, core perceptions should be fully shared. Thereafter, the extent to which cooperation takes place and the way it takes place will depend on the degree of shared perceptions.

The second parameter is mutual benefit. It would be very useful to have mutually agreed-upon "benefit metrics." These would be used to assess the utility of the cooperation and for its persuasive defense. If cooperation is a one-way street and benefits only one party, then its future is unlikely to be very strong.

Third, if cooperation is considered vital and of mutual benefit, it needs to be

safeguarded from unilateral termination by the United States because of extraneous considerations. Recent Indo-U.S. history is replete with examples of unilateral action by the United States, and it would be imprudent not to draw lessons from these examples. A successful global strategy against terrorism requires stability and the continuity of cooperative efforts that are bilateral, regional, and multilateral. If cooperation is ever halted through mutual consent, both parties will have residual responsibilities, such as the nondisclosure of shared data, information, and technology to third parties.

Terrorism is becoming more high tech than in the past. Correspondingly, more contemporary tools, techniques, and systems have to be developed and deployed to combat terrorism. These need to be sold to Indian agencies as part of a normal transaction between the two governments. This would be the fourth parameter, and one that has a strong bearing on the theme of this seminar.

It is necessary to mention that strategic cooperation in counterterrorism would be just one element, albeit new and relevant, in bilateral affairs. It is inevitable therefore, that progress in this area of cooperation would be reviewed in the overall context of bilateral ties between the two nations. The fifth parameter is the idea that cooperation should not be held hostage to the overall state of bilateral relations. Bilateral relations have witnessed highs and lows in the last 50 years, and this is inevitable.

A FIRST-ORDER PARAMETER FIT

Assuming that these parameters are adequate for a first-order assessment, what is the degree of compatibility between India and the United States?

Regarding the first parameter of shared perceptions, there is some convergence, especially after the attacks of September 11, 2001. Nonetheless, the level of convergence does not appear to be enough. The United States has raised counterterrorism to the level of a new "exclusivist religion" and has singled out al Qaeda as its target. India, on the other hand, is more bothered by militant tanzeems organizations operating from across the border in Jammu and Kashmir and, occasionally, from other countries. Contacts between al Qaeda and tanzeems in India do not appear to be strong, although Osama bin Laden has mentioned Kashmir along with Palestine and Chechnya in several vague statements.

India does not, and ought not, consider Muslims, in India and abroad, to be terrorists. India also refrains from U.S.-style racial or religious profiling because of its undesirable effect on the country's composite polity and culture. Indeed, until September 11, 2001, scarred the homeland and psyche, U.S. appreciation of, and sensitivity to, terrorist incidents in other countries was weak. Further, U.S. geopolitics and the short-sighted highlighting of fundamentalist-extremist groups such as the Taliban have generated very valid cynicism in India. Dragon seeds were sown in the subcontinent by the United States, but their second- and third-order consequences were ignored. The irony of U.S. support to General Musharraf, a man who tries to stay in favor with both sides, is not lost in India. The priorities of India and the United States, therefore, appear to be quite different, even now.

U.S. policy is strongly perceived by Muslim nations, at the elite and mass levels, as one of singling out Islam. The fact is that many South Asian and Southeast Asian

countries have significant Muslim populations. Muslims in these countries practice a milder and more accommodative version of Islam than is practiced by their counterparts in countries in the Persian Gulf and West Asia. It may be conceded that there is a fringe element of militant extremists in some South and Southeast Asian countries that deserves to be handled carefully, as it has in the past. It must also be conceded, in the same breath, that fringe groups exist in Christianity, Judaism, and some other religions as well. Perhaps the degree of intolerant behavior by these groups is lower, but they indisputably exist. Here again, India and the United States have some points of divergence both in form and in content. These may get in the way of full-fledged strategic cooperation.

Against this background, it may be unrealistic to hope for a higher level of convergence in perceptions between India and the United States. The fit is not tight, it is loose.

In the Indian context, the second parameter of mutual benefit also appears to be a loose fit. In the tidal wave of sympathy after September 11, 2001, many countries, including India, shared an unprecedented amount of normally classified data and information with the United States. There have been indications, if not intimations, that the benefit from this was one-sided and in favor of the United States. Correspondingly, there is reason to believe that the magnitude and direction of information sharing between the United States and other countries have decreased in the post-September 11, 2001, period. This may be due in part to inertia caused by the massive overhaul of the U.S. bureaucracy, its institutional infirmities, and its procedures, but only partly.

Concerning the third parameter, suffice it to say that the United States as a collective entity ought to make up its mind. This is difficult in the best of circumstances, given the nature of its politics, congressional oversight, activist lobbies, bureaucratic infighting, and an overactive media with its own short-term interests. Sometimes, the priorities of presidential administrations shift. When agreements between the United States and other countries are terminated, one constituency or another is blamed, sometimes quite conveniently. This leads to avoidable erosion of international confidence in bilateral arrangements with the United States. There is a clear and present danger in the reliability of the United States. This problem can be addressed only in and by the United States. Strategic cooperation between the United States and India would, thus, depend on U.S. reliability and credibility.

Regarding the fourth parameter, it is possible and permissible to envision two-way advanced technology and system flows (also referred to as high-tech commerce) between India and the United States in research and development, technology development, prototype evaluation, and free-flow production that are mutually beneficial. However, the legacy of U.S. laws and regulations do not inspire confidence that such science and technology cooperation for counterterrorism would bear fruit.

The fifth parameter is the pursuit of common goals in an area that could be encouraged by both countries, as worked out by professionals of a community in India and the United States at an unofficial level. These professionals could quantify how the cooperative efforts are mutually beneficial, and this may be acknowledged by government officials up to a point. Inevitably, others will step in who have the responsibility of calibrating these cooperative efforts within the overall context of bilateral relations. This calibration involves birds of passage in the diplomatic establishment and the political apparatus in both countries. Realistically, progress in

overall Indo-U.S. bilateral relations may contribute to cooperation in counterterrorism only at the tactical level.

17

Can Science and Technology Help to Counter Terrorism?

Richard L. Garwin

There are large contributions to be made by science and technology, ranging from the most basic research on information technology and the action of bacteria and viruses to the need for new understanding of social dynamics and personal motivation in countering terrorism. Many of these endeavors, if successful, could have far-reaching benefits both for the public and for business. These "dual-benefit" activities are very difficult to design and fund. In addition to the benefits, there are serious prospective problems of misuse, manipulation, and the application of the new-found knowledge by terrorists and by states in warfare.

Nevertheless, it is desirable to push ahead, in order to allow the continuation of free and democratic societies in the face of the evolving threats of personal empowerment and terrorist use of technology.

There is also a matter of motivation of those who work on counterterrorism. It is one thing to construct useful, and even beautiful, buildings against the challenges of cost, time, limited space, and within the constraints of gravity, wind, and functionality. It is quite another to incur significant costs and additional design constraints in an attempt to reduce their vulnerability to terrorism and to losses should an attack occur.

In the medical profession, we see similar conflicts. Some people pursue biomedical research in the quest for knowledge and truth, confident that the information acquired will be helpful in some way. Others invent new technology for countering disease, such as the mechanical stents now so widely applied or the imaging technology that permits the acquisition of information to guide treatment, without the cost and hazard of invasive surgery. At the same time, however, medical professionals put significant effort into repairing the damages of knife and gunshot wounds, preventable accidents, and the like. These "missions of mercy" require every bit as much ingenuity, knowledge, and technique as countering or caring for natural disease, but it is debilitating, to say the least, to exercise and expend such resources when the damage has been inflicted intentionally by one human being on another.

Still, people sort themselves out, and those who are willing, and even committed, to do such work deserve to be supported and esteemed by society. In addition, many of

those working in S&T, as in other endeavors, do so as skilled workers who are employed in a system and who produce for their public or private employers what they are asked to do. They are supervised and evaluated and provided with tools independent of whether what they do is of benefit to society or not. Thus, it is the job of society to harness science and technology routinely and of management to give incentives to individuals and organizations to prevent damage from terrorists and to provide mechanisms to inhibit their activities.

Strengthening the design of a building against earthquake does not automatically increase the threat from fire or disease. In contrast, expending resources to eliminate totally (if that were possible) the possibility of damage from blast, knowledgeable terrorists can, without much difficulty, shift their focus to incendiary or biological or chemical attack, or to a building not yet protected. Therefore, a balanced approach is desirable, countering threats that may not be evident or even imminent today, but that may well be the next resort of terrorists.

Given this somewhat negative assessment of the problems in working to counter terrorism, I recognize that India, the United States, and many other countries have enormous human resources and that there will be plenty of people willing to work effectively to counter terrorism. People who do this work understand that they will not be perfectly successful and that it will result only in ameliorating, rather than eliminating, damage from terrorists.

An additional aspect for such research is the recognition that major damage from terrorism results from the analog of "immune response" of society to terrorist acts. Just as there are autoimmune diseases in medicine, so too the response of society to a threat of terrorism can cause more damage than do the terrorist attacks themselves. In light of this, solutions must always be evaluated in terms of the cost they inflict in society. We should tread as carefully as possible in order to minimize the inhibition of freedom and to permit the evolution of democracy and the enhancement of well-being.

These generalities are illustrated by the following discussion.

DISCUSSION

Terrorism disruptive of entire societies unfortunately spans an enormous range, from the familiar "mall" bomber with a vest or a briefcase full of high explosives to chemical or biological weapons terrorism (thus far not experienced to any significant extent), to the disruption of unique bridges or other urban choke points, to the ultimate nuclear explosion or the multiple seeding of a contagious disease such as smallpox.

There can be considerable learning from experience with the first level of damage from individual events. Particularly from the many cases of suicide bombers in Israel, and now in Iraq, we are familiar with the loss of dozens or even hundreds of people to a single suicide bomber. The general approach to protection is, first and foremost, to reduce the number of individuals who are willing to carry out such activities. This entails a careful look not only at the behavior of our society and government, but also at what the government says and at how it is perceived. I will not mention this again, although I believe that it is of fundamental importance.

Relatively simple approaches for the detection of explosives or explosive-carrying

devices come next. These differ according to the damage that might be done by an explosion, although it is extremely difficult to protect against the loss of one, or even a few, human lives. That stands in contrast with the entire U.S. police and judicial system. U.S. society is remarkably free for an individual to cause damage or death, but at the same time, the number of such activities is held down by the promise of detection, prosecution, and punishment. The normal criminal justice system is of little help against the individual suicide bomber, although it can be of significant utility against a structure that organizes suicide bombers.

Strictly protective measures include explosive detection systems (sniffers) at mall entrances, roadblocks or barriers to prevent high-speed access by vehicles carrying large amounts of explosives, and rapid-detection systems for detecting hundreds or thousands of kilograms of explosives in a vehicle. It is particularly difficult to detect and deter explosives carried or driven by suicide bombers, since they will probably choose the lesser goal of blowing up the guard if they are frustrated in their approach to the more lucrative target.

In order to prevent the autoimmune destruction of society by the threat or practice of a modest amount of mall bombing, it is essential for leaders and citizenry alike to put this threat in context. In the United States there were 2.4 million deaths from various causes in 2001. Of these, deaths from heart disease were 700,000; cancer, 553,800; stroke, 164,000; accidents, 102,000; and influenza, 36,000. Among the accidents, some 42,000 were motor vehicle deaths. An appropriate sense of perspective for leaders and the general public is essential if societal disruption out of proportion to the threat is not to degrade the performance of the society and to impair civil liberties and commerce alike.

For instance, the Nuclear and Radiological Threat category of *Making the Nation Safer* includes so-called dirty bombs.[65] These might not be explosions at all, but simple intentional contamination with radioactive materials.[66]

A key point is the identification of the radioactive material, and the characterization of the threat by duration of exposure. If it is cobalt-60, with a half-life of 5 years, even though a substantial fraction of the population exposed for 5 years could be at risk from cancer, controlled evacuation of the contaminated region within a few days or weeks would limit the hazard by a factor of 50 or more. This is consistent with the regulatory approach to environmental hazards such as arsenic and drinking water, for which the regulated limit in the United States is now 50 parts per billion (ppb), corresponding to a lifetime cancer risk of about 1.7 percent. The new limit is to be 10 ppb (reached by 2006), which then corresponds to a lifetime cancer risk of about 0.3 percent. To my mind, this is unacceptably high, but there is also a requirement that consumers be notified of the arsenic level in their municipal drinking supply, so that they can take individual measures if they so wish.

To reduce the threat from radiological dispersal devices, it is highly desirable to implement stricter control and reporting of the millions of sources of intense radioactivity. These are used for radio therapy in hospitals, industrial radiography of

---

[65] National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, D.C. The report is available in PDF format at *http://books.nap.edu/hml/stct/index.html*.

[66] Dirty bombs have been discussed at some length by Henry Kelly and colleagues from the Federation of American Scientists. See: *http://www.fas.org/ssp/docs/030602-kellytestimony.htm*.

heavy thick materials, and food sterilization as well as, to some extent, polymerization of plastics. Three things have to be done. First, opportunities for terrorists to obtain dangerous radioactive materials must be reduced; second, there need to be early warning systems that would detect illicit movement of radioactive materials; and, finally, panic and casualties from any attack that does occur must be minimized.

At the other extreme of nuclear threats is the explosion of a nuclear weapon or improvised nuclear device in an urban environment or in a harbor. I have published some analyses leading to estimates of hundreds of thousands of people who would be killed by the explosion even of a 1-kiloton bomb (about 5 percent yield of the nuclear weapon that destroyed Nagasaki). For a ground-level explosion, many more people would be killed by exposure to the prompt radiation from the explosion and to the immediate fallout of the debris from the explosion itself than occurred in Hiroshima and Nagasaki.[67]

Protecting society against terrorist use of nuclear weapons lies in the improved safeguarding of nuclear weapons by the states that possess them. In this regard, Russia is a special problem in view of the tens of thousands of nuclear weapons and the rather poor security created by the economic problems in that country. Pakistan is another concern, because its dozens of nuclear weapons are at risk of diversion by sympathizers with extremist Islamic groups, and also by a potential coup against the government.

It is possible to detect the nuclear materials – Pu-239 or U-235 – most commonly used for nuclear weapons. Of these, highly enriched uranium is the greater problem, since it is far less detectable than plutonium. Uranium is also easier to fabricate into a nuclear weapon that might well have the full yield of the Hiroshima bomb – some 13 kilotons.

Another general-purpose instrument against terrorism is intelligence. To this we need to add the powerful tool of appropriate financial rewards for informants.

Turning to bioterrorism, I offer three examples: foot–and-mouth disease, salmonella, and smallpox.

Foot–and-mouth disease (FMD) is a highly contagious disease that affects pigs and cows. It is not apparently a threat to human health. However, it is typically forbidden to import any animal product from an infected region into a country free of FMD because it is so contagious. This is a problem that cries out for improved vaccines, in order to prevent the spread of FMD in places where it already exists, and to protect animal populations in states that are free of FMD. Ironically, the existing vaccine is not much used for protection because its use results in the animals developing antibodies that cannot be distinguished from the presence of FMD.

It is in the interest of the trading nations of the world to develop effective protection against FMD, and this could very well be done in India. More effective vaccines for FMD are needed. It is highly desirable to carry out such work, even though the United States has been free of FMD. As with smallpox, the absence of even a single case should not convey a sense of security, but a profound sense of insecurity and instability against the introduction of the disease.

Salmonella is a frequent cause of food poisoning in the United States and to a greater extent in other countries. Its cause is a common bacterium causing primarily illness and occasionally death. The one recorded bioterrorist incident in the United

[67] Garwin, Richard. August 19-24, 2002. "Nuclear and Biological Megaterrorism," *27th Session of the International Seminar of Planetary Emergencies,* Erice, Sicily.

States, other than the anthrax attacks of fall 2001, was by the Rajneeshee sect in Oregon that wished to reduce the number of people voting, in order to give their candidate a better chance of being elected.

We have had a lot of recent experience with anthrax. Among our new-found knowledge is the effectiveness of antibiotic treatment after symptoms begin. To recapitulate, anthrax forms a hardy spore, which survives in the environment for decades. When it is ingested in the lungs or gastrointestinal tract, some fraction of the spores enter the vegetative state, from which the bacteria can reproduce.

There is an effective vaccine against several strains of anthrax, and as mentioned, there is also effective antibiotic treatment. However, recent knowledge of the mechanism by which the bacterial population produces disease implicates three protein products of the bacteria. These toxins act in specific ways in animal cells. These actions can be blocked by appropriate chemical counters. Should such a treatment prove viable, there would be another approach besides preventing the disease or preventing the multiplication of the bacteria, and that would be to detoxify the toxic products, so that the disease itself would be less harmful to its host. Much more biomedical research along these lines is indicated. India should be a prime location because of the substantial competence of its scientists and the lower cost of doing research there.

Despite the effectiveness of a few grams of anthrax in killing five people, it is not highly communicable. In principle, therefore, improved hygiene can protect individuals from the primary source, and it is not necessary to take strong measures to isolate people sick with anthrax.

Smallpox is different. We all know that the world has been free of smallpox since the World Health Organization (WHO) made an extraordinary effort to eradicate the disease worldwide. This was possible because smallpox has no animal hosts other than humans.

In 1972, the U.S. government terminated its vaccination program. Arguments in favor of termination included the fact that several people per year died of side effects of the vaccine, and no one died of smallpox. Therefore, why vaccinate?

Vaccination against smallpox is the analogue of permanently inserted control rods in a nuclear reactor. Failing substantial vaccination, the country is at risk to the dissemination of the smallpox virus. If, for example, the virus were disseminated at a busy airport, tens of thousands of people could unknowingly be exposed and disperse it throughout the United States and the world. In the 2 weeks or so that it takes for the disease to become apparent, many others would be infected, but the key point is that the number of people infected would continue to double or triple every 2 weeks after that.

Smallpox has a fortunate characteristic in that vaccination is effective during the first 4 days after exposure, or so it is thought. Therefore, it is possible in principle, with an appropriate distribution of vaccine and a few-minute course in vaccination techniques, for a few thousand workers throughout the United States to create 10,000 effective vaccinators in the first hour and many times that in the second hour, so that all reachable individuals could be vaccinated within a couple of days. Such an effort would require a plan and provision of bifurcated needles and other supplies for the vaccination process.

The United States has been largely unsuccessful with the George W. Bush administration's initiative to vaccinate large numbers of first responders and health-care workers, and to make vaccination available to those who desire it. I believe this is a

significant failure. Further, there is not yet a plan to vaccinate hospital and emergency workers in a single day.

My August 2002 paper describes the effectiveness of nonspecific measures to counter a smallpox epidemic.[68] Smallpox is not among the most highly communicable diseases. Experience with natural epidemics indicates that each smallpox victim infects about three others. Hence, 1,000 primary cases would grow in 2 weeks to 3,000. Two weeks later that number would grow to 9,000, and so on. If the transmission could be reduced by a factor of 4 – to an average of 0.75 secondary cases per primary case – even if there were no other treatment, 1,000 primary cases would result in a total of 4,000 cases altogether, rather than in tens or hundreds of millions of deaths.

Society need not set up quarantine or other barriers routinely, but they should be available if an outbreak of smallpox (or Severe Acute Respiratory Syndrome [SARS]) occurs, at the first sign of a significant number of cases. This would do nothing for the primary victims, but it would keep a tragedy from becoming a disaster by limiting the infection to a multiple of the initial cases, compared with the potential millions of victims of a fulminating epidemic.

In order to achieve this level of containment there must be analysis and planning. In addition, implementation of a plan would require action by much of society. This can only be achieved by the distribution of action messages via radio and particularly television. The Internet is an excellent distribution medium in the United States because it provides data on demand; following an alert, anyone with Internet access would be able to access and print the information relevant to their locality. In instances of biological terrorism, a radiological dispersal incident, or the release of toxic material, the channels for distribution of warning and action information to the public are not inherently affected. Simultaneous attacks on the Internet and the power grid would, however, amplify greatly the impact of biological weapons, radiological dispersed devices, or chemical attack.

EPILOGUE

Science and technology specific to countering terrorism includes the means of ensuring premature detonation of explosives or of inhibiting the triggering of explosives. Most science and technology counterterrorism tools are highly useful for public health, law enforcement, or general intelligence purposes. Much science and technology now useful for counterterrorism is embodied in systems in general use, such as the media of mass and selective communications. Science and technology cannot eliminate the problem of terrorism, but they can help in opposing it.

[68] "Nuclear and Biological Megaterrorism"

18

Discussion of Indo-U.S. Cooperation

T.G.K. Murthy and John Holdren,
Discussion Moderators

The presentations by K. Santhanam and Richard Garwin were followed by an extensive discussion of steps that might advance Indo-U.S. cooperation in applying science and technology to combating terrorism. The discussion moderators in this session were T.G.K. Murthy and John Holdren, who both discussed opportunities and pitfalls; the subsequent discussion attempted to narrow down the subjects for cooperation, but also noted political and other obstacles.

Murthy began by reiterating the commonalities between India and the United States: they are the biggest democratic countries in the world, and they have a shared faith in human freedom, which is sometimes exploited by terrorists. The manifestations of terrorism will be different at different times and are highly unpredictable. Murthy regarded terrorism as an effect, but what is its cause? The mitigation of terrorism requires a holistic approach, not a single-point solution. There must be sensors, surveillance systems that operate from different platforms, stretching from the ground to elevated platforms, to space-bound systems. Murthy expressed his surprise that space technology had been ignored in the workshop's discussion. Space technology plays a vital role in society and in the world as a whole; there is a potential for terrorist activity to spread to space programs.

Murthy asserted that a key element in combating terrorism is information-gathering systems that act as eyes, ears, and intelligence, for which there should be newer materials such as biomaterials and nanomaterials, appropriate process technologies, and maybe some body-embedded microelectromechanical systems (MEMS), perhaps for security guards assigned to important figures. He suggested that MEMS-based systems could be embedded into bridges, high-value systems, highways, and even nuclear platforms, and monitored from space-based surveillance systems. They could be complemented by high-resolution thermal vision systems, which the workshop had not considered. Murthy concluded by reiterating the problem, discussed earlier by Santhanam and P. Rama Rao, of the difficulty of exchanging information between states because of walls of laws, embargoes on technology, and so forth.

Holdren tried to organize the problem of applying science and technology into different tasks, and these might be undertaken in different fora. One task is that of "sharing and comparing." The two countries could share and compare perceptions, practices, experiences, and analytical results relating to different threats and responses. They could also share and compare technology, designs and hardware, and intelligence.

A second approach would go beyond sharing and comparing. It would involve the joint analysis of threats and responses and codesign of strategies, laws, and regulations. It would also involve working together to develop, improve, and test technologies; to build individual and institutional capacity; to educate the public and policy makers; and to implement the identification of actual emergent threats, and the interdiction and defense against them in recovery from attacks if they cannot be prevented. There would also be joint work to conduct what Holdren called "integrated assessment" of an area of terrorist threat and response; for example, what does the whole landscape look like, what more could be done, what are the unexploited opportunities, what are the areas where resources are being wasted, what are the areas where resources are inadequate? Those are all forms of joint work that could be envisioned.

Next, there was the practical question of how the two countries would interact and cooperate. Is it best done with ad hoc workshops, lab-to-lab working parties (of the sort that had taken place between the United States and Russia on such problems as nuclear materials protection, control and accounting, and, briefly, between the United States and China)?

Other forms of interaction include standing joint committees for oversight and analysis (such as an existing committee within the National Academies and Russian Academy of Sciences for oversight and analysis of U.S.-Russian cooperation on nuclear nonproliferation and counterterrorism). There are also joint centers for analysis and technologies, and various joint operations for implementation, identification, interdiction, defense, and recovery.

Another way to characterize these kinds of cooperation is by asking who organizes them? What are the organizing entities, academies, think tanks, universities, national laboratories, and institutes, for example, the Indo-U.S. Science and Technology Forum, the Nuclear Threat Initiative, and various combinations of United Nations' agencies, such as the International Atomic Energy Agency (IAEA)? Holdren noted that in his paper he had applied this framework to develop an architecture for actual and potential forms of Indo-U.S. cooperation on nuclear threats.

Holdren noted that this was the moment to start thinking systematically about recommendations for cooperation. He added that there is the further issue of relevant criteria; that is, we need to identify the intersection points between the most dangerous threats and the most compelling opportunities. It is particularly important that the subject chosen should have some chance of delivering helpful results quickly: it does not make sense to pick important problems that were close to impossible to solve.

Two interventions from earlier discussions were especially relevant to the question of selecting topics for joint U.S.-India research. Marco DiCapua suggested that there might be separate matrices for India and the United States—the weight that the threat represents, the ease or difficulty of implementation, and the strength of each country to engage in dealing with that threat. There might be activities where India has strengths that would greatly benefit the United States and vice versa. For the United

States, one would rate the importance of communications and information technology (IT) very highly, and give a very low weight for difficulty; agriculture and biotechnology would be important, but slightly more difficult, whereas for nuclear safety the weight of importance would be very high, but so would the weight assigned to the difficulty of coping with the problem. Thus, disease and pathologies in cattle would be an excellent theme for collaboration, because there are some big asymmetries in the cattle industry in the United States and India, and the cattle industry has such a large economic importance when one cow with bovine spongiform encephalopathy (BSE) disease can have a major impact on U.S. industry, as recently occurred. Similarly, for India, cattle are important for agriculture and for protein production.

The safety of nuclear installations and the response to nuclear disasters has already been vetted by the U.S. Inter-Agency Group. From the U.S. perspective this is easy to do; whether India will agree is an open question. Other joint projects could involve nuclear materials protection, control, and accounting; exchange of best practices; and techniques for surveillance of e-mail and Internet networks.

M.K. Rasgotra proposed a nongovernmental meeting of 20 or 25 countries that have nuclear assets or have a potential of acquiring them. He suggested that the United States could meet with two, three, or four similarly placed countries and discuss the nature of their safety measures. Similarly, India could assemble a different group of two or three countries to discuss safety issues, and then these six or eight states should come together. After a few years the group could be enlarged to 20 or 25 countries.

Rasgotra advocated such a group because events had bypassed the Nuclear Non-Proliferation Treaty, the IAEA, and the Nuclear Suppliers Group (NSG), which he termed a "denial group." The NSG had to be converted to a "nuclear safety group." There might also be a consortium of nuclear plant builders to develop a standard design, and evolve standard safety practices, and pool expertise to develop cheaper alternative sources of energy for countries that cannot afford civilian nuclear plants. Rasgotra concluded by observing that unless there was a world organization or facility that collectively devised means of providing cheap, affordable, nonnuclear energy to such countries, this race for nuclear power will continue.

Roddam Narasimha reiterated that while there was agreement that the terrorism problem is not the same in the United States as it is in India, there are many areas where the two countries might be able to work together—and identifying these areas is important. He restated the criteria for selection of joint projects that had been proposed by Ambassador Harry Barnes in an earlier session. Barnes had offered six guidelines for selecting cooperative projects: (1) prioritize a few feasible projects, with deadlines for completion, (2) assign specific responsibilities to each side, (3) identify and confirm funding sources, (4) establish clear channels of communication, (5) flag potential obstacles, and (6) remain aware of what the two governments were doing. He also suggested that Indians and Americans, when working together, are apt to be very ambitious, which is good, but were sometimes ambitious to the point of being unrealistic, and Barnes urged that the criteria be "MA" or "AM": modestly ambitious or ambitiously modest.

Christopher Davis suggested five initial criteria for a joint Indo-U.S. project that applied science and technology to the problem of terrorism: (1) mutual interests, (2) individual strengths, (3) complementary requirements, (4) nonsensitive issues and, (5) mutual benefits.

Narasimha stated that funding should not be a problem if good topics were chosen; he judged that the best Indian partner for such a joint project was not the Indian Academy of Science but one of the national laboratories or institutes. He agreed with earlier speakers that there were still sensitivities in both countries, and that an early failure would damage the chance for continued cooperation.

Nuclear reactor safety was an area of strong common concern. So were projects that drew upon Indian strengths in IT, both in academia and in the private sector. India was also strong in matters connected with surveillance, sensors, and sensor technology development, and was very interested in electronic interceptors, jammers, and technologies related to surveillance. Further, one interesting possibility is sharing experiences with power transmission, where India is in the peculiar position of having a system that is so bad that it has learned to live with it. There may be lessons for others, notably the questions of islanding, analyzing transmission, and grid management, which are noncontroversial and seem to be promising areas for U.S.-Indian collaboration.

Kumar Patel suggested that proposals for collaboration fell into at least five categories, that is, software-based activities, nuclear facility security, personnel identification, sensor networks, and biosecurity, and perhaps others.

A potential software project is database development and integration, which is important when information is incomplete. The task is how best to organize such a database, how to integrate it to find what we are looking for with a high level of probability. Other software-related projects might include what Patel called Internet surveillance software, which, by monitoring Internet traffic, might enable the discovery of connections between various groups. There also is the general area of cybersecurity and computer modeling of contamination and cleanup to achieve maximal cost-effectiveness. Another software-related challenge is to measure the norms of behavior across networks, so that we can better distinguish bad activity from good activity, and use cyberintelligence to help enforce laws.

The problem of nuclear facility security raises political sensitivities, but it is important to protect these facilities from terrorist attacks; getting the right language that would allow this type of cooperation is something that intelligent people can work on.

In the area of personnel identification and authentication, Patel noted that it was evident that inexpensive biometrics both for identification and for authentication would help enormously. It would also help for access control to nuclear and other sensitive facilities, specifically for reducing the level of potential terrorist threats to these installations.

Sensors and sensor networks, whether of people, motion, or vibration, may be something on which both countries can work. The United States and India have a shared problem of illegal aliens crossing borders. Can we do something together even if there is little or no terrorist implication for securing the U.S. border? The real issue is, can you beneficially construct an inexpensive network or a cost-effective network to do what you want to do?

In the area of biosecurity, perhaps some sort of a disease surveillance system might help distinguish naturally occurring outbreaks from intentionally caused diseases—an Indian equivalent for agriculture of the U.S. Centers for Disease Control and Prevention.

Finally, there are such issues as the protection of transmission networks against electromagnetic pulse terrorist threats, and physical attacks against the grid infrastructure.

DiCapua noted that there already was a proposal from the U.S. National Nuclear Security Administration to discuss nuclear emergency management, although he noted that there had not yet been a response from the Indian Atomic Energy Commission. Further, the Defense Attaché Office has discussed the idea of cooperation in installing sensors along India's borders; in addition, there already was a joint program in which India and the United States collaborated on the development of vaccines. Finally, India has tremendous experience in pulse vaccinations, vaccinating millions of people in a short time.

Several Indian participants reminded the group that there were still obstacles to cooperation on terrorism-related issues. Narasimha noted that President George W. Bush and Prime Minister Vajpayee had announced an agreement the previous day, but expressed caution about early expectations for major collaborative efforts at the official level. He suggested the possibility of collaboration with the Safety Research Institute of the Indian Atomic Energy Regulatory Board (AERB); this might supplement other official channels.[69] Narasimha pointed out that historically there had been much skepticism in the Indian energy and space sectors regarding collaboration with U.S. counterparts, and that the United States had not even provided technology that would enable India to examine cracks in pressure vessels. K. Santhanam cautioned that whatever is undertaken should be kept simple, and that there had been numerous technology exchanges that failed, or in some cases, U.S. technologies were unsuitable for Indian circumstances. New technology applications must consider local conditions, and the Indian experience with some U.S. remote monitoring systems in the past was that they were not applicable to Indian conditions.

Richard Garwin also offered two cautions: (1) There may be structural problems with collaboration. Some U.S. organizations may be competitive with Indian ones, unless they found that working together provided a competitive edge. (2) There were cases where the technology was developed by intelligence agencies, or funded by them, and in such cases (for example, jamming or premature detonation of explosives) it is extremely unlikely that there will be any sharing of the information.

Continuing in the same vein, Lawrence Papay and others noted the sensitivity of data mining of Internet or cell network surveillance. The U.S. government and the National Security Agency want to close-hold such technology, so this may not be an area for genuine bilateral partnership. He and others also noted the sensitivity of the problem in terms of laws and civil liberties.

To this, Raja Menon suggested that many terrorists caught in Southeast Asia and in India have confessed to extensive use of the Internet. He was unsure of the U.S. view, but asked whether concerns over fundamental rights could prevent us from looking at the Internet when the terrorists use it extensively for their command and control and to

[69] In 2006, the AERB status was changed and put under statutory control.

execute their operations. Lewis Branscomb responded that this is a lively issue in the United States, and that any joint Indo-U.S. project would have to include an analysis of the legal and philosophical views of different countries—this was not just a technical issue.

Seymour Goodman, who had developed a group at Stanford University that combined legal and technical expertise, suggested that the prospect of cyberlaw, which would make it a serious crime to attack information systems, computer communication systems directly, or to use them to attack other things, was worth exploring. Such laws are notably lacking worldwide, and an Indo-U.S. team might work together to develop such laws. These issues involve not just lawyers, but require a lot of technical talent to write laws that are workable, protect civil liberties, and establish a legitimate international baseline. This would be noncompetitive, there could be a clear point of achievement, and it would have a short time line. Above all, these laws are necessary, not in the least to provide the basis for extradition. The need is for a congruent set of laws that essentially agree on what is a serous crime. Without such laws, even very advanced technology may not be enough.

DiCapua noted that the U.S. Legal Law Attaché in New Delhi was working on cyberterrorism issues, yet the lack of a body of law in India to deal with computer terrorism was a real obstacle in working together. A seminar of lawyers and technical people who can discuss these matters would be a strong addition to two cultures that are based upon the rule of law. Narasimha noted that the National Institute for Advanced Studies in Bangalore has worked intermittently with a group of academics from the National Law School University (Bangalore), and there are some firms in Bangalore that specialize in legal issues connected with computers. Branscomb noted that he was planning a collaboration with an Austrian computer scientist and lawyer on the subject of piracy and security, and agreed that law-technology-terrorism was a very realistic project, certainly requiring the deep participation of technical experts.

Goodman agreed, and emphasized that writing such laws, and getting them adopted, would be a strong form of closure, perhaps a model for other countries.

N. Balakrishnan noted that the legal and political sensitivities regarding the Internet and cyberterrorism are especially important in the United States. When India tried to find out more about a U.S. Internet service provider (ISP), the U.S. response cited its privacy laws, and the need for a subpoena, with the result that nothing much happened. He also noted U.S. sensitivity on such issues when Admiral Poindexter was required to change the name of a Central Intelligence Agency program from Total Information Awareness to Terrorist Information Awareness.

Menon noted the difference in U.S. and Indian vulnerabilities to cyberterrorism and the Internet, pointing out that the United States has an infrastructure, which is so developed that it can be attacked by cyberterrorism, but India does not, at least for now. He pointed out that there was already a task force in operation between India and the United States on legal cooperation in law enforcement, under the joint chair of the National Infrastructure Protection Center (NIPC) and the Indian Intelligence Bureau (IB). These would be the "customers" for a joint Indo-U.S. study. The immediate problem for Indians is not their vulnerability to a cyberattack, but the use of the Internet by terrorists, and using it to attack them.

Narasimha suggested that the next step would be to turn to the Indo-U.S. Forum on Science and Technology to support a few small expert workshops to develop specific projects from among those discussed at this workshop. Patel agreed, and suggested that these workshops focus on three major areas: biometrics and related bioproblems, data mining and fusion, and the general area of nuclear safety. These seemed to be the subjects on which there is consensus and expertise.

In discussing biometrics, there was agreement that it is important to distinguish between cooperative or joint studies of biowarfare and the spread of disease through animal and plant populations on the one hand, and developing technologies by which biological indicators could be used to verify individual identities on the other. The latter might have application in many fields, including nuclear reactor safety. There were also possibilities of developing cheap diagnostic tools, or sharing expertise in biological weapons cleanup or mass vaccination. Christopher Davis noted that the United States was eager to reach agreement with other countries on biometrics.

There were some dimensions of data management that did not fall afoul of civil liberties, or involve comprehensive sifting of communications intercepts, an approach that raises political issues. As Branscomb noted, this is the area of sensors and networks. While the National Academies' report[70] says that there is plenty of work on sensors, there is an inadequate understanding of how to manage thousands of sensors spread around when some have been destroyed, some give false positives, and some give false negatives. How, for example, would a mayor interpret the data that does come in? This is a very sophisticated computer science and logic problem that might involve both U.S. and Indian scientists.

As for nuclear and reactor safety, a participant pointed out that work on biometrics—developing authentication systems—could be a dual-use application for security access to sensitive nuclear facilities. Such a system would enable the monitoring of workers as they moved from plant to plant and keep track their total accumulated dosage. Santhanam noted that for a physical security program involving radioisotopes, we must also determine where the greatest area of seepage is—from the former Soviet Union or some other country—and what is likely to be the target, a country in the West or India?

Rose Gottemoeller suggested that, building on her understanding of U.S.-Russian cooperation, the United States and India could work together to establish a regional training center in India for security best practices. This would not force the issue either bureaucratically or institutionally, or raise concerns, such as premature access to facilities. The experience with the Russian strategic rocket forces did turn out to be an appreciable confidence-builder.

Narasimha concluded the workshop by outlining four sets of issues that seemed to be of great concern to both countries:

1. IT-related problems and processes, including software, data mining, knowledge management, and analyzing vast amounts of data from sensors

[70] National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, D.C. The report is available in PDF format at *http://books.nap.edu/hml/stct/index.html*.

2. biometrics and biomedical research and development, including perhaps agriculture-related diseases
3. a cluster of surveillance-related issues, with an overlap between some kinds of biometrics and human surveillance
4. nuclear safety, possibly with the involvement of the Indian Safety Research Institute and the Atomic Energy Regulatory Board