India-United States Cooperation on Science and Technology for Countering Terrorism: Summary of a Workshop

ISBN
978-0-309-31296-7

184 pages
6 x 9
PAPERBACK (2014)

Rita Guenther, Micah Lowenthal, and Lalitha Sunderesan, Rapporteurs; Committee on India-United States Cooperation on Science and Technology for Countering Terrorism; National Academy of Sciences; in cooperation with the National Institute for Advanced Studies, Bangalore, India

India–United States Cooperation on Science and Technology for Countering Terrorism

Summary of a Workshop

Rita Guenther, Micah Lowenthal, and Lalitha Sundaresan, Rapporteurs

Committee on India-United States Cooperation on
Science and Technology for Countering Terrorism

NATIONAL ACADEMY OF SCIENCES
THE NATIONAL ACADEMIES

In Cooperation with the National Institute for Advanced Studies
Bangalore, India

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

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract/Grant No. S-ISNCT-12-CA-1003 between the National Academy of Sciences and the U.S. State Department. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-31296-7
International Standard Book Number-10: 0-309-31296-5

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, NW, Room 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; 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 J. 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. C.D. Mote, Jr. 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. Victor I. Dzau 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 J. Cicerone and Dr. C.D. Mote, Jr. are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

.

NATIONAL RESEARCH COUNCIL COMMITTEE ON INDIA-UNITED STATES COOPERATION ON SCIENCE AND TECHNOLOGY FOR COUNTERING TERRORISM

Norman R. Augustine (NAS, NAE), *Chair*, Retired Chairman and Chief Executive Officer, Lockheed Martin Corporation
Penrose (Parney) Albright, Associate Director at Large, Lawrence Livermore National Laboratory
John Holmes, Deputy Executive Director of Operations, Port of Los Angeles (former)
Nancy B. Jackson, Manager, International Chemical Threat Reduction Department, Global Security Center, Sandia National Laboratories
Randall S. Murch, Associate Director, Research Development Team, National Capital Region, Virginia Tech
Nancy Jo Nicholas, Associate Director for Threat Identification and Response, Los Alamos National Laboratory
George Perkovich, Vice President for Studies and Director, Nuclear Policy Program, Carnegie Endowment for International Peace
Stephen P. Cohen, Brookings Institution (retired), *Consultant*

National Research Council Staff

Rita S. Guenther, Study Director
Micah D. Lowenthal, Director, Committee on International Security and Arms Control
Wei Jing, Research Associate

NATIONAL INSTITUTE FOR ADVANCED STUDIES COMMITTEE ON INDIA-UNITED STATES COOPERATION ON SCIENCE AND TECHNOLOGY FOR COUNTERING TERRORISM

V. S. Ramamurthy, *Chair*, Director, National Institute of Advanced Studies, Bangalore, India
Manoj Bali, Director, Directorate of Low Intensity Conflict, Defence Research and Development Organisation, New Delhi, India
H. V. Batra, Director, Defence Food Research Laboratory, Mysore, India
S. Chandrashekar, Professor, Indian Institute of Management, Bangalore, India
S. Gopal, Government of India, retired
Rajaram Nagappa, Program Head, National Institute of Advanced Studies, Bangalore, India
Gulshan Rai, Director, CERT-In (Indian Computer Emergency Response Team) and Group Corrdinator, Cyber Law Division, Ministry of Communications and Information Technology, New Delhi, India
Anuradha Reddy, Director of Personnel, Ministry of Defence, New Delhi, India
A. K. Sinha, Senior Research Officer, National Disaster Management Authority, New Delhi, India
Lalitha Sundaresan, Visiting Professor, National Institute of Advanced Studies, Bangalore, India

Preface and Acknowledgments

The governments of India and the United States initiated a bilateral Homeland Security Dialogue in May 2011 with a visit by then U.S. Department of Homeland Security Secretary Janet Napolitano to meet with former Indian Minister of Home Affairs P. Chidambaram. The 2011 meeting marked the first comprehensive bilateral dialogue between the two countries, which was established to "strengthen the global strategic partnership between the United States and India on issues ranging from cybersecurity and megacity policing, to counterterrorism and countering violent extremism."[1] The dialogue is a mechanism by which the two countries reaffirm their commitment to work cooperatively on law enforcement issues, combat common threats, improve bilateral cooperation through the development and application of innovative technology, combat the flow of illicit finances and currency counterfeiting, and to work closely to counter terrorism and promote cybersecurity. Further, the Homeland Security Dialogue facilitates the identification of "areas in which the United States and India can collaborate on science and technology development and its application in the homeland security context."[2]

India and the United States are the world's two largest democracies, with distinguished scientific traditions and experts in a wide range of scientific-technical fields. Given these strengths and the ability to learn from one another, the U.S. National Academy of Sciences (NAS) together with the National Institute for Advanced Studies (NIAS) in Bangalore, India, held a joint Indian-U.S. workshop to identify and examine potential areas for substantive scientific and technical cooperation that can support cooperation and counterterrorism efforts through the Homeland Security Dialogue and through direct cooperation. The workshop agenda included biological threats (health and agriculture); protection of nuclear facilities; security (physical and cyber) for chemicals, chemical facilities and other critical infrastructure; and monitoring, surveillance, and emergency response. To accomplish this, NIAS and NAS convened technical experts from India and the United States to begin discussions about science and technol-

[1]Department of Homeland Security. "Readout of U.S.-India Homeland Security Dialogue." Available at http://www.dhs.gov/news/2013/05/21/readout-us-india-homeland-security-dialogue; accessed July 25, 2014.

[2]Ibid.

ogy to counter terrorism, and to identify promising opportunities for India and the United States to learn from each other and cooperate in these critical areas. The workshop was hosted by NIAS from February 3 to 5, 2014, and built upon a successful NAS-NIAS joint workshop held in Goa, India, in 2004, which produced a report entitled, *Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop*.[3] One decade later, the 2014 workshop summarized in this report underscored the extent to which experts from India and the United States have increased their cooperation as well as the tremendous opportunities that remain for further joint efforts.

In preparation for the workshop, NAS formed a planning committee comprising prominent scientists, engineers, and a South Asia expert. The planning committee members and NAS staff worked collaboratively with scientific and technical experts in India, NIAS leadership, and staff counterparts to develop the agenda for the workshop. During a planning trip taken by NAS planning committee members and staff in August 2013, the two groups met and refined the agenda, identified potential speakers, and determined other elements of the workshop. In addition, NIAS and NAS organizers met with key officials in the government of India, who provided their support for and input to the workshop. The workshop itself enabled Indian and U.S. experts to describe their work and plans for future activities on a breadth of scientific and technical areas relevant to counter terrorism.

The following summary intentionally includes a large portion of the material discussed during the workshop to provide readers with extensive insights into the views of the Indian and U.S. participants. The challenges they described are faced by both the United States and India, and both nations have much to learn from the exchange of information and experiences to increase security, efficiency of operations, and the safety of employees, location populations, and the environment. As a result, the technical approaches detailed here will be of interest to many readers. For those readers interested in a high-level overview of the workshop discussions, key messages and promising topics for collaboration arising from the presentations and discussions have been pulled out in the Synopsis.

The U.S. Department of State funded NAS participation in this workshop, with supplemental funding from the Patel Endowment to the NAS. NIAS provided substantial financial support for the workshop by providing housing and meals for participants, as well as providing the facilities and administrative and technical support for the workshop. The generous support of all sponsors is greatly appreciated.

This report is a factual summary of the presentations and discussions at the workshop, and does not provide consensus findings or recommendations. The

[3]National Academy of Sciences. *Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop*. Washington, D.C.: The National Academies Press, 2007. Available at: http://www.nap.edu/openbook.php?record_id=11848; accessed October 24, 2014.

key issues and selected thoughts on goals and opportunities for collaboration noted in the synopsis at the beginning of the report are some of those raised by individual workshop participants, and do not in any way indicate consensus of the workshop participants overall.

This report has been prepared by the workshop rapporteurs as a factual summary of the presentations and discussions at the workshop and does not provide consensus findings and recommendations. The planning committee's role was limited to planning and convening the workshop. The key issues and selected thoughts on goals and opportunities for collaboration noted in the synopsis at the beginning of the report are some of those raised by individual workshop participants. Those statements, and any other views presented in the report, are those of individual workshop participants and do not necessarily represent the views of all workshop participants, the planning committee, or the National Academy of Sciences.

We wish to thank the following individuals for their review of this report: Ravi Grover, Homi Bhabha National Institute; John Holmes, U.S. Coast Guard (Retired); David Kaufman, Federal Emergency Management Agency; Vivek Lall, General Atomics; Michel O'Brien, Lawrence Livermore National Laboratory; Amy Sands, Monterey Institute of International Studies; and Jeffrey Starr, Neo Prime Solutions, Inc.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the content of the report, nor did they see the final draft before its release. The review of this report was overseen by Mona Dreicer, Lawrence Livermore National Laboratory, appointed by the National Academies, she was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the rapporteurs and the institution. Technical experts of both India and the United States, as demonstrated during this workshop, seek opportunities to work together on issues related to counter-terrorism. While the task of addressing such a broad range of terrorist threats is vast, so too is the experience and expertise available in our two countries to meet this challenge. Joint efforts such as this workshop provide the basis for India and the United States to continue to learn from each other, to exchange ideas for collaborative efforts, and to increase the confidence and support necessary to take their cooperation further as they work to counter terrorism in their respective countries and around the world.

Contents

Synopsis

The terrorist attacks of September 11, 2001, in the United States and the terrorist attacks in Mumbai on November 26, 2008, significantly increased attention paid to the complexity of threats to safety and security around the world. Recognizing shared concerns, capabilities, and willingness to cooperate, the governments of India and the United States initiated a bilateral Homeland Security Dialogue in May 2011 with a visit by U.S. Department of Homeland Security Secretary Janet Napolitano to meet with Indian Minister of Home Affairs P. Chidambaram. The dialogue, which continues today, is a mechanism by which the two countries reaffirm their commitment to work cooperatively on law enforcement issues, to combat common threats, to improve bilateral cooperation through the development and application of innovative technology, to combat the flow of illicit finances and currency counterfeiting, and to work closely to counter terrorism and promote cybersecurity.[1]

To facilitate cooperation on science and technology to counter terrorism via the Homeland Security Dialogue and directly, the U.S. National Academy of Sciences and the National Institute for Advanced Studies (NIAS) organized and convened a workshop entitled "India-U.S. Workshop on Science and Technology for Countering Terrorism," held February 3-5, 2014, in Bangalore, India, on the NIAS campus. The plan for the workshop is described succinctly in the statement of task in Box S-1.

GOALS AND OBJECTIVES FOR JOINT WORKSHOP

The workshop itself enabled Indian and U.S. experts to describe their work and plans for future activities on a breadth of scientific and technical areas relevant to countering terrorism, including Systems Approaches to Countering Terrorism; Security at Chemical Facilities; Agricultural and Food Security; Technical Aspects of Civilian Nuclear Material Security; Global Health Security and Strengthening

[1]Department of Homeland Security. "Readout of U.S.-India Homeland Security Dialogue." Available at http://www.dhs.gov/news/2013/05/21/readout-us-india-homeland-security-dialogue; accessed July 25, 2014.

BOX S-1 STATEMENT OF TASK

An ad hoc organizing committee under the auspices of the National Academy of Sciences (NAS) standing Committee on International Security and Arms Control (CISAC) will work with partner organizations in India to convene an Indian-U.S. workshop on science and technology for countering terrorism. The organizing committee and its counterpart in India will develop the workshop agenda, select and invite speakers and discussants, and moderate the discussions. The agenda will include topics to address biological threats (health and agriculture); protection of nuclear facilities; security (physical and cyber) for chemicals, chemical facilities and other critical infrastructure; and monitoring, surveillance, and emergency response. It will also include topics to identify and examine promising areas for further Indian-U.S. cooperation on science and technology for countering terrorism.

Public Health Infrastructures; Emergency Management and Response, An All Hazards Approach, Protecting Critical Infrastructure; Cybersecurity in its Complexity; the Challenges of Conventional Terrorism; and Forensics Capabilities during Response Phases, Attribution, and Perpetrator Prosecution. Overarching themes that emerged from the detailed discussions, and outlined thematically here in the synopsis, were the need to develop, test, and implement systems of security; the tension faced in India and the United States between the core mission of companies or research institutions and the needs of safety and security; similar tensions among free speech, privacy, and security in open, democratic societies; and the need to prioritize among a variety of domestic and international terrorist threats.

KEY ISSUES FROM WORKSHOP

The key issues noted here are some of those raised by individual workshop participants (names shown in parentheses) and do not in any way indicate a consensus of workshop participants overall.

- **Focus on the overall security objective:** To determine how best to design, test, implement, and operate a fully functional system of security that addresses evolving terrorist threats, it is valuable to define the overall security objective, and then to identify the needs and actions based on subsidiary objectives that are linked to and consistent with the overall objective (Nehchal Sandhu and Norman Augustine).
  - A systems approach, from vulnerability assessment to life-cycle analysis, considering how all of the security pieces fit together helps avoid common failures. Likewise, testing of all of the pieces as a system at the time of installation and reassessing and retesting over

time help to avoid unsuccessful security procurements (Byron Gardner and John Holmes).
  - Examining terrorism as a systems problem means in part prioritizing vulnerabilities, prioritizing the value of assets, and prioritizing choices. By doing this, the effect of terrorists may be reduced (Sandhu).
- **Science and technology have roles in countering terrorism:** Not only can science and technology offer particular solutions to individual or collective security challenges, the scientific and technical communities can serve as a resource for decision-makers at all levels—from the individual facility level to the national governmental level—and can inform assessments, procurements, implementation, standards, oversight, testing, and continual reevaluation (Sandhu, Vinay Kajla, K. Sekhar).
  - Several participants noted a need to develop additional mechanisms whereby the government of India and the United States can discuss the challenges of counter terrorism with scientists and technical experts. In India, participants noted there is a need for mechanisms whereby independent scientific advice can be provided to the government as it seeks to address evolving terrorist threats. In the United States, while several mechanisms exist for receiving scientific advice, there are parts of the government that would benefit from greater scientific expertise and insights (Sandhu, Augustine, David Franz, Nancy Jackson, Raymond Jeanloz, Van Romero, Gardner, Keshav Kumar, R. P. Sharma).
  - Similarly, there is a need for the scientific community to be more aware of terrorism challenges as they arise so that they may be in a position to provide more effective proposed solutions (Sandhu, J. K. Bansal, B. J. Srinath, B. Karthikeyan).
  - While there are a variety of industries and companies that have expertise and technologies that may be helpful in counter terrorism efforts, these industries rarely have an overall view of the threats. As a result, efficiencies are difficult to realize in terms of expertise, equipment, and innovative input into possible solutions (Gardner, Michael O'Brien, Karthikeyan, Kumar).
- **Technology may be part of the solution, but human components are essential:** It is not possible to regulate all potential threats away. The results of scientific and technical research can be beneficial as well as potentially harmful creating what is often called the dual use dilemma. Given this reality, it is not possible to entirely eliminate risk, making the need to build trust globally and to work together even more urgent and essential. Enlightened leadership, a culture of personal and corporate responsibility, and leaders who are willing to take responsibility to develop thoughtful regulations and safe and sustainable practices, and maintain freedom for scientists to explore, would facilitate progress for all people in, for example, the life sciences and those who rely on their beneficial work (Sandhu, Augustine, Franz, Karthikeyan, Jeanloz).

  - The most important breakthroughs in investigations of terrorist incidents often come from classical hard police work that included data and information analysis rather than from extraordinary technologies (Jeanloz, Franz, Kajla).
  - When one looks at an integrated systems-level response to an incident, the human aspect is an essential component. Just because one has technology does not mean the problems are solved. Without properly trained people, even the best systems cannot succeed in providing the best possible security (O'Brien, Gardner, Kajla, Kumar).
  - Quite often, high-cost, sophisticated security systems fail because their component parts are not integrated with each other or with the larger system in which they need to operate. At times, less may be more, in that purchasing the most expensive or elaborate systems may not always result in the best and most effective security systems. Facility operators, an experienced participant noted, usually do not understand the capabilities and limitations of the security systems; this includes operators at government and private facilities. There is often a need to change the culture and mindset of operators and facility owners so that security is seen as necessary and becomes a norm (Gardner, O'Brien, Karthikeyan, Kumar).
- **The importance of the primary work and functions of facilities is critical:** While it is difficult to do so, it is essential to find a balance between investments in security and investments in the fundamental mission of the facilities, which is science and technology. (Jeanloz, Franz, L. V. Krishnan).
  - Over-investment in one area to the detriment of the other jeopardizes the overall mission of the facility and/or security (Augustine, Jeanloz, Sandhu, Jackson).
  - Similarly, a balance needs to be maintained between the interests of security and the interests of society in terms of civil liberties and privacy (Jeanloz, Augustine, Sandhu, Kajla, V. S. Ramamurthy).
- **Capacity building to address both natural hazards and malicious acts may increase through cooperation:** There is tremendous expertise and experience at local, state, and national levels in India and in the United States that can be harnessed to address natural and man-made hazards (Nancy Jo Nicholas, Karl Kim, Kajla).
  - This includes human and other resources that may have been allocated for one set of disasters, but which can be utilized in preparing for, responding to, and rebuilding from a range of incidents (Kim, Kajla).
  - Training and communication with local communities will allow the knowledge and expertise of local residents to be harmonized with overall strategies for an all-hazards approach to incident prevention and response (Kim, Kajla).

  - There is a need to move away from "fail safe" to "safe to fail" approaches. Since it is not possible to entirely eliminate the risk of natural disasters and malicious acts, it is important that critical infrastructure and facilities remain safe to people and the environment even if their operations fail. For example, with sea-level rise, more areas will inevitably be flooded, requiring us to rethink zoning or no-build zones (Kim).
  - Responding to emergencies, whether accidental or man-made, requires the coordination of a large number of agencies, organizations, and groups. If these agencies learn to cooperate and integrate, many problems in emergency management and response can be solved. Failing to coordinate can result in inefficiencies of human and financial resource allocation, disempowerment of local communities, and confusion in incident preparedness and response. Coordination of groups in advance of an incident would ultimately have reduced the loss of life, property, and infrastructure. Experiences with emergency responses in the United States have indicated the benefits of these improvements over time (Kajla, Kim, Romero, Kumar).
- **Protecting critical infrastructure is important to the resiliency of communities, economies, and societies overall:** Chemicals, the products of biological research and production, civilian nuclear materials, and information technologies are essential for any modern economy (Jackson, Karthikeyan, Franz, Srinivas Mukkamala, Srinath).
  - Almost all products on the market today started from chemicals. As a result of their importance, it is not possible to lock chemicals away as one can secure uranium or plutonium (Jackson).
  - In addition to the need to protect chemicals, a participant noted that there is a need to protect chemistry expertise, such as expertise in making illegal drugs, making chemical explosives, or using chemicals to make weapons (Jackson, Karthikeyan).
  - It is not possible to control all biological equipment and technology. It is not possible to control knowledge. It is not possible to isolate scientists. It is not possible to know all of the biohackers who may be out there. However, it is possible to build awareness and understanding (Franz).
  - Cybersecurity is a real priority for industries and for critical infrastructure protection. Cyberthreats cannot be dismissed as coming from amateur hackers working in seclusion to create mischief, noted a participant. Therefore, it is essential to incorporate cybersecurity into a systems approach to security overall, and should not be isolated (Augustine, Jackson, O'Brien, Gardner, Holmes, Jeanloz, N. Balakrishnan, Srinath, Romero).
  - For all infrastructure, it is important to preserve the proper functioning of critical systems to the greatest extent possible in the event of an incident (Kajla, Kim, Jackson, B. K. Maurya, O'Brien, Gardner).

SELECTED THOUGHTS ON GOALS AND OPPORTUNITIES FOR COOPERATION

The selected thoughts on goals and opportunities for cooperation noted here are just some of those raised by individual workshop participants, and do not in any way indicate a consensus of workshop participants overall.

- **Monitoring and surveillance**
  - Joint development of improved technologies for monitoring and surveillance in difficult–to-observe locations such as areas of high foliage and high altitude, through walls, around corners, or in remote areas may be mutually beneficial (Sekhar).
  - Maritime Domain Awareness is particularly well suited for collaboration given the significant potential threats that may arise along the coasts of the United States and India. Improved situational awareness will also improve security at ports and other areas of passenger and cargo transport, and may provide additional areas of cooperation (Holmes).
  - Many participants noted that the application of surveillance should be balanced in free, democratic societies, and open dialogue is an essential aspect of the development of relevant technologies (Jeanloz, Augustine, Sandhu, Kajla, Ramamurthy).
- **Prevention of weapons acquisition**
  - Reducing the use of high-risk materials, securing higher-risk material inventories by establishing trusted networks in industry (explosives and chemicals), prompt reporting, and real-time monitoring are important to the prevention of weapons acquisition (Jackson, Karthikeyan).
  - Insider threats, including sabotage, should be taken seriously, stated several participants, and training would be an effective and efficient means of beginning discussions on this topic (Ravi Grover, Jeanloz, Krishnan, Augustine, Jackson, Vedpal Yadav, O'Brien, Gardner, Holmes, Mukkamala, Srinath, Romero, Sekhar).
- **Physical security for infrastructure**
  - Focus on training and technical and nontechnical solutions and testing, performance assessment, and evaluation may be useful areas for India-U.S. cooperation (Sandhu, Augustine, Holmes, Karthikeyan, Gardner, O'Brien, Holmes, Romero, Sekhar, Sharma).
  - Monitoring and modeling of critical infrastructure are incomplete at this time, including for food security; chemical, biological, and nuclear security; cybersecurity; and for more traditional infrastructure such as bridges, airports, and shipping lanes. Cooperation in these areas may be beneficial to experts in both the United States and India (Sandhu, Augustine, Franz, Yadav, Jackson, Karthikeyan,

Grover, Krishnan, Ramamurthy, Jeanloz, Bansal, Nicholas, Kim, Holmes, Maurya, O'Brien, Gardner, Mukkamala, Srinath, Kumar, Romero, Sekhar, Sharma).

- **Cybersecurity**
  - There are several means by which experts from India and the United States may be able to effectively cooperate in the area of cybersecurity, including by sharing best practices through training (Balakrishnan, Mukkamala, Srinath).
  - Legal frameworks, standards, and oversight are in their infancy in the area of cybersecurity, and a wide range of stakeholders and experts (including those in private industry) may effectively be convened to propose paths forward in these areas (Balakrishnan, Mukkamala, Srinath, Jeanloz).
  - Development of technologies that are more resistant to cyberattacks will be increasingly important and, given the expertise in both India and the United States, collaboration would be mutually beneficial (Sandhu, Augustine, Jeanloz, O'Brien, Gardner, Holmes, Sekhar, Romero, Balakrishnan, Srinath, Jeanloz).
- **Emergency preparedness and response**
  - Assessment of vulnerabilities and planning solutions, including community-based actions, would be helpful to both countries (Augustine, Kajla, Kim).
  - Increased resilience is needed in both the United States and India, and by sharing best practices for building community and institutional resilience, as well as physical resilience, much could be learned (Kim, Kajla, Sandhu, Augustine, Gardner, O'Brien).
- **Forensics and attribution**
  - Focusing on training and establishing the scientific basis for the reliability of the many tools and techniques that may lead to increased attribution capabilities is a potentially fruitful area of cooperation (Sharma, Romero, Kumar).
  - While there are many technologies in existence and being developed, the scientific and evidentiary basis for conclusions drawn from various forensic techniques and technologies still need to be established and scrutinized and made available to those who make decisions based on this evidence (e.g., the court system) (Sharma, Romero, Kumar, Franz).
- **Science and technology advice and interaction**
  - Sharing of mechanisms for obtaining scientific and engineering advice and assessments, and for connecting operational needs with scientists and engineers who develop tools, could benefit both the United States and India (Sandhu, Augustine).
  - Incorporating scientific and technical expertise into the decision-making processes can be effective in the areas of response and pro-

active technology development. Further, involving the scientific and technical communities in decision making can provide a means of coordination across disciplines and areas of expertise, increasing the opportunity for maximizing innovation, efficiency, and effectiveness (Sandhu, Augustine, Kim, Kajla, Jeanloz, Franz, Bansal, Maurya, Srinath, Kumar, Romero, Sekhar, Sharma).

BUILDING ON THE SUCCESS OF THE WORKSHOP

Technical experts in a variety of fields associated with science and technology to counter terrorism provided presentations and engaged in frank discussions. These experts were chosen by the workshop organizers from the national laboratories, academia, and nongovernmental organizations of their respective countries. Over the course of the three-day workshop, they provided their perspectives, knowledge, and experience and shared ideas for possible future joint collaborations between India and the United States. Participants expressed their hopes that cooperation and collaboration on common problems would arise from this first step at sharing about the science and technology needs. The workshop was not intended to provide a particular plan of action or specific concrete next steps for this collaboration. Rather, it was intended to bring forth a variety of areas in which experts from the two countries can proceed with cooperative efforts in their areas of expertise based on identification of mutual goals and priorities. In subsequent phases of engagement, more specific topics may be identified and appropriate time and resources may be devoted to sustained and intensified cooperation.

1

The Realities of Terrorism in India

V. S. Ramamurthy, co-chair of the workshop planning committee, opened the workshop by welcoming all those present, which included those who had traveled from New Delhi, Mumbai, and the United States as well as the faculty and students of the National Institute for Advanced Studies. He stated that the goal of the workshop was to openly and frankly share experiences and expertise and to consider areas of potential cooperation between Indian and U.S. scientific and technical experts to address the significant challenges of countering terrorism. International terrorism remains a compelling challenge, not only for India and the United States, but also for many other countries and regions of the world. Given the high caliber of scientific and technical experts gathered at the workshop, Ramamurthy stated that there was no doubt that jointly tremendous progress can be made.

Ramamurthy introduced the keynote speaker, Deputy National Security Advisor Nehchal Sandhu, to explain the nature and scope of the terrorist threats India faces.

CHALLENGES OF TERRORISM IN INDIA

Nehchal Sandhu professed that Indian practitioners, for more than 30 years, have not had sufficiently wide and deep interactions with the scientific community of the country. Sandhu therefore dedicated some of his remarks to what he perceived as the current gaps in countering terrorism and what he believes the scientific community can do to assist.

Sandhu underscored Ramamurthy's remarks regarding international terrorism as a compelling challenge and the possibility that its burgeoning profile is going to affect larger sections of the world community. Sandhu noted that, in the Indian context, the level of terrorist violence has been consistently decreasing. While that is a good sign, he also admitted that terrorists still retain the capacity to strike hard, to strike at will, and to carry out incidents that result in mass casualties. The November 26, 2008, attacks in Mumbai resulted in a loss of more than 100 lives in a multi-scene attack that persisted over 3 days until the challenge was surmounted. Even as the numbers of incidents have decreased in India, Sandhu stated that there was an awareness of the reality that the ugly face of

terrorism could arise anywhere and precipitate incidents that result in mass casualties with all of the attendant issues that they create for the government to address.

Sandhu, during his remarks, limited his assessment of the current situation and the reality of terrorism in India to the two most vital theaters from the government's perspective. The first is Jammu and Kashmir, which has been the venue of terrorism since 1989. The second is terrorism in the northeast, where it has been festering longer. In both cases, there is a significant external factor contributing to the tensions. The forces or groups that carry out terrorism in India, or in Jammu and Kashmir specifically, are not exclusively focused on India. There is a need for the world community to take note of the fact that the same forces pose terrorists threat in many other parts of the world. Sandhu said he was tempted to recall that when the Joint Working Group on Counterterrorism with the United States first met in 1999, India's assertions about the threat of Lashkar-e-Taiba to the American mainland was met with disbelief, until then U.S. Coordinator for Counterterrorism Michael Sheehan began to understand input from India. U.S. experts began to take note of the extensive Lashkar documentation that existed indicating a threat to the United States. There have been a few cases where Lashkar has been directly implicated in conspiracies on the American mainland in addition to what they have been doing in theaters in India.[1]

Sandhu noted that he does not believe the thesis that has been put forth by some quarters that Lashkar is a franchisee or a subordinate group of Al Qaeda. Ideologically, there is no way in which the two could come together. Al Qaeda in India is not as well organized with cohorts and outfitted as Lashkar. The numbers of Lashkar adherents is significantly higher. Denominationally and ideologically, there is no meeting ground between Al Qaeda and Lashkar.[2] That said, he believes we need to pay attention to the fact that Lashkar has adopted the program of global jihad.

Sandhu strongly urged members of the American delegation to take note that this single organization, which today has a membership of about 3,500 to 3,700 people is the next big threat to the world. Soon after it came into being in the mid-1990s and the early 2000s, evidence came to light of Lashkar activity in Iraq, Chechnya, Dagestan, and Kosovo.[3] Lashkar withdrew from those territories for good reason, to reinvigorate and reassemble its capacities. Over the last 2.5

[1]Members of a Virginia jihad network had provided material support to Lashkar-e-Taiba (LeT), and the Muridke camps of LeT, near Lahore, was used as a hideout for Mir Aimal Kansi, convicted for killing Central Intelligence Agency officers in January 1993.

[2]Steve Cohen pointed out that he does not know of any credible sources that argue that LeT has a close relationship with Al Qaeda. That may have been true in the first years of LeT and Al Qaeda, but Bruce Riedel, Steven Tankel, and others have argued that they are quite different organizations.

[3]Padukone, Neil. "The Next Al-Qaeda? Lashkar-e-Taiba and the Future of Terrorism in South Asia," *World Affairs Journal*, November/December 2011. Available at: http://www.worldaffairsjournal.org/article/next-al-qaeda-lashkar-e-taiba-and-future-terrorism-south-asia; accessed October 24, 2014.

years, a significantly enlarged presence of Lashkar has been seen in the eastern provinces of Afghanistan, namely Kunar and Nuristan. These are only serving as a holding ground and as platforms for actions farther westward into other parts of Afghanistan, and more specifically as a means of targeting Kabul over a period of time. Some of these attacks have been carried out by Lashkar independently. Others have been carried out in conjunction with groups like the Haqqani Network. Sandhu noted that the westward mobility established by Lashkar indicates that it has designs much larger than one might have expected. Although there are many other terrorist groups, he does not think that any other group represents the kind of threat that Lashkar does.

Sandhu praised the U.S. designation of Lashkar as a terrorist group and the continuing efforts, including U.S. Treasury Department efforts, to ensure that finance channels that sustain the operatives of Lashkar are systematically disrupted. All of that continues to restrain plans to extend Lashkar's jihad to global proportion.

Sandhu then discussed Jammu and Kashmir and shared figures that might reveal the situation more clearly. In 2001, there were 3,504 terrorist incidents resulting in approximately 1,520 casualties in Jammu and Kashmir. In 2013, there were 113 incidents with 15 casualties. This reflects significant success by the security forces in dealing with this challenge. Another clear indicator of progress is that from a high number of 3,700 terrorists in the province of Jammu and Kashmir, there are now only 429 terrorists. This also indicates that there has been significant attrition and that the capacity of Lashkar to rejuvenate and to reinvigorate in Jammu and Kashmir has to a large extent been impared.

Two broad strategies have brought benefits in Jammu and Kashmir. One is the erection of a physical obstacle, a fence, along the Line of Control (LoC) and the international border in the state. The second is the deployment of high-tech surveillance devices, whether those are hand-held thermal imagers, long-range observation systems, battlefield surveillance radars, unmanned aerial vehicles, or other devices. There is a diverse combination of equipment and material on the ground to try to maintain the integrity of the fence and to detect every effort made to cross it. Notwithstanding these efforts, Sandhu indicated that every year 300 to 400 terrorists try to cross the fence and about a hundred were successful. The government estimates that in 2013, 97 terrorists managed to get through. This occurs mostly due to the heavy snow and ice that blankets some areas to depths of 4 to 5 meters, covering and in some places mangling the 3.3-meter fence. People attempting to cross have to be adept at ice-craft and snow-craft, which means the numbers of successful attempts in winter is limited. When the snow and ice recede, approximately 30 percent of the fence must be rebuilt each year at considerable cost. More importantly, it takes a month or two to re-erect the damaged fence, leaving areas exposed for some months.

The existing multifaceted approach to detecting and neutralizing terrorists within the state of Jammu and Kashmir consists of three broad elements. First, there is what in India is called a Counterterrorism Grid, which means the territory of the state of Jammu and Kashmir has been mapped onto a grid. Each section

of the grid has been assigned to specific units to patrol, and units collaborate across the grid elements. The second part of the program consists of intelligence-driven operations. Whether that intelligence is acquired by technical means or by human sources, there is an ability to act quickly on intelligence. That is how losses are inflicted on terrorist groups, Sandhu stated. Third, there has been a sustained campaign to ensure that people whose normal activities are circumscribed by violence perpetrated by terrorists are not only liberated from that stranglehold, but are also able to pursue their avocations and participate in India's democratic traditions, for example, by becoming members of the legislative assembly. Through legitimate elections, voters elect people who can justifiably and appropriately represent the interests of the people and seek recourse and remedies to address concerns and grievances through legitimate means rather than through violence.

Shifting to the northeast states, there were 1,076 incidents in 2004 with approximately 500 casualties. In 2013, there were 732 incidents with 107 casualties. Sandhu noted that the number of incidents was reduced by only 25 percent in 10 years. Casualties, however, were reduced by 75 percent, which is a significant advance. The four states where there are issues of concern are Assam, Manipur, Meghalaya, and Nagaland.

Sandhu stated that different counterterrorism strategies have been pursued in different areas. For example, in Nagaland and Assam, there have been dialogues with terrorist groups for a long time. As a result, for example, in Assam, today there are 21 autonomous councils. They cover specific jurisdictions wherein peoples' representatives are largely from the ethnic group of that particular area. The councils have the capacity to decide where to apply development funds, and where they want to allocate other money that becomes available: to build roads or schools, or for some other purpose. That has been one part of the model. The other part has been a joint command including the army and the paramilitary forces to deal with the threat as it emerges in different areas.

While there has been some success, when the government "settles" with one group and invests elected representatives from that group with power, there may be a remnant group that remains deprived of the gains of office. This leads to reoccurrences of insurgencies. The Bodoland territory is one example, where, over a period of 15 years, three sets of people have engaged in an insurgency, and this is still a persistent problem. Sandhu admitted that he is uncertain whether elected representatives of people on these small councils are ultimately the answer. Simultaneously, police actions and paramilitary actions have continued, and that has led to some reduction in the number of casualties and a greater degree of security.

In Nagaland, talks have been held with one of the factions of the Nagaland Socialist Council, the Isak Muivah faction, for more than a decade. As a result, violence has been reduced, although other groups do not feel constrained and have continued with some degree of violence. The struggle for supremacy between the various groups leads to fratricidal killing (killing of people in one's

own group) as opposed to killing of civilians (killing of those from other groups). This is a different kind of violence.

Here, too, it is important to mention that external factors help drive these forces of terrorism. The availability of territories in Bangladesh and increasingly in northern Myanmar has provided these groups areas of sanctuary where they can regroup. These are platforms through which funds can be collected and funneled into territories in India. These are areas where weapons acquisitions occur. In late January 2014, a Bangladeshi court convicted 10 people, including Paresh Baruah, [4] for having attempted to bring 10 truckloads of weapons into India.[5] Another area of interest is the southern Chinese state of Yunnan, not very far from Myanmar. Sandhu stated that there is ample evidence of Indian insurgents headquartered in and around Myanmar, Taga, and Naga Hills taking shelter in a place called Ruili, which is just across the border in China on the road to Kumming.

Sandhu provided another example of the connection to external forces. About 2 or 3 years ago, Anthony Shimray, a Naga insurgent, went to Thailand and contracted with gunrunners for the delivery of several million dollars' worth of weapons for which he had paid a million dollars in advance. An investigation by the National Investigation Agency exposed the plot and he was intercepted; today he is the subject of prosecution in court in Delhi. Further, 161 AK-47 rifles were smuggled recently in three different tranches across the Myanmar border into Nagaland. The rifles were a part of the weapons purchase initiated by Anthony Shimray.

A third matter Sandhu addressed in regard to Lashkar is what has been termed the Indian Mujahidin. There have been reports in the press about this group causing terrorist acts. The leader of this group, Yasin Bhatkal, was arrested, and prior to that, Saudi Arabia repatriated Zabiuddin Ansari.[6] It is important to note that while these people are clearly Indian nationals and they have no foreign background, each one of them has been taken to Pakistan, usually through a third country in the Middle East and sometimes even through Iran to Pakistan, trained in camps there and then sent back to carry out terrorist acts inside India. What is also more interesting is that this has happened more than once. It is not just a matter of being taken there, trained, and then sent back. Guidance flows from nodal points in Pakistan through clandestine communication channels about selection of targets, timing of attacks, positioning of weapons and hardware, the supply of money, and other aspects. There is an estab-

[4]Baruah is the chief of one Assam's insurgent groups.

[5]Allchin, Joseph and Victor Mallet. "Bangladesh Court Sentences 14 to Death for Huge Weapons Haul." *Financial Times*, January 30, 2014. Available at: http://www.ft.com/cms/s/0/0cebf490-89af-11e3-abc4-00144feab7de.html#axzz3H61620SF; accessed October 16, 2014.

[6]Zabiuddin Ansari is an Indian national and an Islamic fundamentalist belonging to the Indian Mujahidin and LeT, and has been accused of involvement in the 2008 Mumbai attacks.

lished externality, a key component outside of India, in the way in which the Indian Mujahidin group is able to carry out its activities.

Sandhu then turned to the issue of where science and technology experts—like those at the workshop—can possibly play a role in assisting the state apparatus in dealing with terrorism. First, in India, much of the identification of potential terrorist recruits, their enlistment and motivation, takes place on the Internet. Most of the recruits are younger people who understand how to use the Internet. Of the 1.2 billion people in India, there are 243 million Internet subscribers, 42 million of them use broadband service through land lines and the remaining approximately 201 million users are on mobile platforms. Most of the mobile platforms are patronized by youth who use them for social networks like Facebook and Twitter. There is a segment of the population that uses these networks for nonpeaceful pursuits. There are chat rooms, for example, that remain exclusive to people who are swayed by a certain kind of ideology. They tend to have entrenched radical positions and this sometimes translates into terrorist activity.

It remains a challenge for law enforcement agencies to keep track of what is happening in real time on the Internet, in chat rooms, and elsewhere. One of the reasons is, unlike in America, the Indian government is not permitted to monitor all of the traffic that occurs. Government agencies are permitted under law to approach authorities to obtain warrants for specific targets. Sandhu stated that the government cannot just suspect someone of doing something harmful and monitor that activity. Law enforcement agencies must identify targets to be monitored and request warrants that may or may not be granted. Once approved, the warrants are subjected to a system of review. Therefore, there is quite a challenge in securing warrants, and even when the suspected traffic is monitored, law enforcement is unable to decipher some of that traffic. As a result, the government remains unaware of all of the radicalizing activity that is taking place on the Internet. Internet-based human sources, where agents and operatives masquerade as X or Y individual, enter groups, and help to take sites down are not permitted in India, unlike in the West. Indian law does not permit law enforcement to conduct such sting operations.

Another area of concern is communication, broadly defined, including not only the Internet, but also IP-based radios and cellular data networks: global system for mobile satellite communications (GSM) and code division multiple access. In the radio frequency spectrum where GSM networks of a neighboring country are being spread into India through high-powered external transmission and reception networks, much of the traffic is not in the voice domain, but in the data domain. Discussion is necessary for defining an approach to address the challenge posed.

Decoding encrypted traffic remains a challenge, particularly with regard to specific conspiracies that rapidly progress. Sandhu recounted that about 3 years ago, Indian authorities recovered a device that was like a small calculator, a keypad, attached to a very high frequency (VHF) radio. The keypad had Arabic letters on it, and users would enter their messages in Arabic, then the little key-

pad would encrypt the message and send it out in burst mode through the VHF radio. Sandhu shared the device with his Indian colleagues and with the U.S. Central Intelligence Agency. After more than 2 years, they still do not really know how that device worked. Innovative designs like this continue to appear, which defeat efforts to monitor what is occuring.

Another significant domain in need of scientific and technical assistance is that of explosives. Sandhu noted that there are three specific areas where they have difficulty. The ability of terrorists to use common materials to fabricate bombs—glycerin, soap, ammonium nitrate, potassium chlorate, sulphur, charcoal, etc.—makes it difficult to prevent such bombs. Sandhu was not certain if scientists could help with detection of explosive devices made out of these materials. They realize that even though these materials can be easily obtained and mixed, the detonation mechanisms are not as readily available. They require controlled materials such as an electric detonator or a detonator at the end of a fuse wire.

That said, Sandhu noted that they have had difficulties in tracking detonators. Detonators are issued for legitimate purposes, such as in mining and blasting rock for building roads. India lacks a means of going back to the last point of sale of detonators. Indian experts are able to trace if they had been manufactured by a certain company, if they had gone to a certain state, but after that point it is not possible to trace them to the end user. They are hoping to acquire a mechanism whereby each detonator can be tracked all the way from manufacturer to user. Second, detonators in explosives are often linked by a common wire to a battery some distance away and when someone presses a switch to cause the detonation. With timers, terrorists are able to distance themselves from the site of explosion. There are timing delays, not just on the electronic detonators but even on physical, manual detonators. It is not always possible to be precise when it comes to a detonation mechanism of that type, but they have been used in the past.

Light-dependent resisters (LDR) can also be programmed as detonators. They can be put into a room such as a conference room, for example. When someone comes in and turns the lights on in the morning, the mechanism would be activated, and 40 minutes later or in 1 hour, for example, the device would detonate. Conversely, at times terrorists construct the mechanism to cause an explosion when darkness decends. LDRs are another effective means of separating the perpetrator from the event. Other cases include loosely termed solar-powered rockets. These are rockets that are placed roughly 4 to 5 kilometers from the target. Again, there can be a device similar to an LDR. As sunlight reaches a certain level, a rocket would be triggered. Usually such devices are quite inaccurate, but they do have a fairly lethal capacity even when they are off their mark.

Cellular phones and wireless sets are also used as triggers. They are now more sophisticated than original designs where the mere establishment of a carrier or a ring was sufficient to detonate a device. Today, there are devices in which detonation will not occur until communication has been established and a

four- or six-digit code has been entered. It is not unusual for terrorists to wait for an army convoy to approach to establish the connection and then wait until the intended target approaches to enter the code and detonate the device. Thus far, Sandhu stated, security agencies have not been able to develop effective ways of detecting the presence of such a device or defeating it. For example, they would like to operate a vehicle that can send out a barrage of frequencies at sufficient strength to cause a device to detonate far in advance of those who may be approaching. There is a third part of the physical aspects of explosives that needs to be addressed. Terrorists have begun to create shaped explosives like claymore mines to direct the maximum fury of the device in a certain direction. For example, recent Indian Mujahidin bomb blasts were created from a wooden boat-shaped structure. The structures are lined with metal and then filled with explosives following the boat's shape. Ball-bearings were placed in front and a detonator was placed in the back and with a timer. When the blast occurred, shrapnel flew in a certain direction. Copper-backed shapes are also used to launch the maximum impact of the explosive in a certain direction. Booby-trapped bodies are another means of delivering a detonation that causes significant challenges. When someone is killed and the body is booby-trapped, anyone who comes to inspect the body can be blown up in a secondary explosion.

India has cooperated with the U.S. Joint Improvised Explosive Device Defeat Organization (JIEDDO) on detection of improvised explosive devices (IEDs), below ground and elsewhere. Sandhu stated that the two or three programs conducted with JIEDDO did not provide a satisfactory means of detecting and disrupting IEDs dug into roads 2 or 3 feet below ground. It was not possible to detect any of these devices. There is insufficient emission of vapor for detection, and the metallic parts are too deep for even a deep-search metal detector to detect a device.

Sandhu raised another challenge to which they have not yet found a solution. Terrorists have dug tunnels in at least three instances under the LoC. These tunnels are typically 3 to 4 meters underground and are usually 1.5 meters high and about 1 meter wide. They run approximately 700 to 800 meters, starting approximately 200 meters on the other side of the LoC and extend 500 meters into the Indian side. Two broad techniques have been tried to disrupt this tactic: ground-penetrating radar and conductivity tests, neither of which has been successful. Although there are strong defenses on the surface (e.g., good fences), there is no apparent solution to the challenge of deeply burrowed tunnels.

Sandhu described areas where India has conducted significant research. One such area is on increased equipment reliability. Recently, in Central India, there have been several cases where helicopters used for casualty evacuation, for flying commanders from point A to point B or for flying policemen from point A to point B, have been struck by adversary weapons at critical moments which bring them down. There have been cases of hydraulic failure, and cases in which the tail rotor has been blown off. There have also been cases of fuel tank puncture. A program has been initiated to protect these helicopters by bullet-proofing critical sections of the helicopter. Unfortunately, vulnerabilities remain.

Sandhu noted that there is yet another area, a relatively soft area, where terrorists have done a great deal in terms of using technology for harmful purposes: the replication of travel documents, identity papers such as election ID cards, drivers licenses, and passports. The high quality of the counterfeiting makes these false documents very difficult to detect. He noted that they have tried four or five ways of embedding security features into these documents, some of which have worked, while others of which have not. Certainly, this is an area where solutions are urgently needed.

Another area of concern that Sandhu noted is the poisoning of the water supply, which has been declared as an intended target by terrorists. There have only been two cases thus far. Fortunately, in both cases the quantity of cyanide put into the water was too small, and therefore, it did not create the kind of impact that the perpetrators were intending. Therefore, detection of even small qualities of poisonous substances, not only cyanide, in large volumes of water available for consumption is needed.

In closing, Sandhu stated that radiological dispersal devices, so called dirty bombs, are also of concern, although there have been no such incidents in India. This is another area where India will need a great deal of assistance and cooperation from the scientific and technical communities because it is quite a challenge.

Sandhu then concluded his prepared remarks and stated his willingness to answer questions from workshop participants.

DISCUSSION

Norman Augustine, co-chair of the workshop planning committee, began by thanking Sandhu and noting that his remarks were sobering due to the magnitude of the challenges faced in India. He asked a question about the progress and success in reducing casualties caused by terrorism in India and in the United States. Did Sandhu notice a difference in the threat or in the nature of the activities as India has been more successful at interdicting terrorists? Have they changed the nature of their attacks?

Sandhu replied that he was referring to the counter-terrorism grid that was established in Jammu and Kashmir in conjunction with the army and paramilitary forces. Essentially, what the grid does is rid the populated areas of terrorists. They have to move away into the upper reaches and away from civilian pockets. If the civilians and terrorists can maintain that separation, they are reasonably certain that terrorists would not have the capacity to conduct a mass killing. That is what they concentrate on.

Once the terrorists are driven into the hills, there are fewer civilians amongst them and the ability to engage terrorists without causing collateral damage is much better. However, they continue to identify means of creating problems. For example, it is not unusual for them to use surrogates or unsuspecting collaborators to cause harm. They may fabricate an explosive device packed in an innocuous item

such as a transistor radio and tell an innocent person that it needs to be given to a specific person for repair, asking that person to deliver the item. Upon delivery, the radio blows up. There is very little one can do about these incidents. Police try to keep changing their tactics such as setting up checkpoints for detecting the material that comes into civilian areas, but terrorists continue to innovate such that they can get around whatever devices are erected to prevent terrorist acts.

R. Narasimha thanked Sandhu for his informative account of the terrorist problems in India, especially those that demand solutions in the realm of science and technology. There was a similar India-U.S. meeting 10 years ago, and at various times discussions with American and Indian colleagues have been held about these issues. What mechanisms are there in India to discuss these problems with scientists and technical experts and not necessarily within the government?

Sandhu replied that sadly there is no such mechanism. When M. K. Narayanan was the director of the Intelligence Bureau, he established a mechanism whereby there was a Technology Group within the Bureau that had representatives from all over. They had then taken up something very interesting with the Defence Institute of Psychological Research about "what makes a terrorist," looking at a large body of material collected over a period of time, and very worthwhile work resulted.

There is obviously a case to be made to reviving a forum for the exchange of ideas where at least the practitioners of counterterrorism can bring their problems forward and put them on the table and have the scientific community address those issues. There are many bilateral discussions, but nothing like a platform, for example. **Prof. Balakrishnan** is assisting with big data analytics and sentiment analysis. This is all one on one, which is not necessarily the only way to proceed.

Sandhu stated that he was just struck by another possibility regarding science and technology integration into counterterrorism efforts. The National Knowledge Network (NKN) will soon become a reality, connecting 1,562 institutions within the country; 1,003 have already been connected.[7] The NKN permits the creation of communities that facilitate collaboration across geographies on a given subject. Maybe Indian experts could suggest to R. Chidambaram, Principal Scientific Advisor (PSA) to the Prime Minister, and Professor Raghavan that a closed group be created on the NKN where counterterrorism practitioners could pose problems, and those with capacities to address the challenges could log in, see the problems, and select problems with regard to which they could assist. There would be money within the PSA's office to finance such activities. Perhaps this is a model that could help.

A workshop participant strongly seconded the proposal and added that it is certainly possible for this type of group interaction via the NKN and that it should certainly be pursued.

[7]For more information about the National Knowledge Network, see: http://www.nkn.in/; accessed September 11, 2014.

Sandhu replied that he thinks the biggest advantage of this kind of a group would be flexibility, because different sets of skills are needed, and one does not necessarily need to have a permanent set of people at one place for solving all problems.

Sandhu agreed that there are some very interesting experiments of this nature that have taken place in India. There is an annual event at IIT Delhi where one can see new technologies on display. Technologies that could help, and programs are initiated with those who developed the technology. Notably, one of them was low power transmitters to be left on unattended buoys in the sea. They had other applications too. Another example was video analytics being done in the Bharti (2) Building. What Sandhu noticed at IIT Delhi of particular interest was what they called the Technology Business Incubation Unit. Some technologies identified 10 years ago have spun off into successful enterprises. A company called Kritikal is an example; they created an automatic number plate recognition device. They created underbody cameras for detecting devices. Now they have come to the stage where they are a credible independent company. That is a huge success story. Certainly, there is a need for the scientific community to at least be aware of the problems. A workshop participant then asked if there are any laboratories in India that specialize in forensics and technology for counterterrorism.

Sandhu noted that there are a number of very, very good labs. For example, most of the computer devices and other computer media or mobile phones seized from terrorists receive the best imaginable examination at the Forensic Science Laboratory in Hyderabad. In terms of voice matching, Gandhinagar is impressive. In terms of DNA analysis, the Center for Cellular and Molecular Biology, Hyderabad is extremely good. In terms of explosives, Madhuban Forensics Laboratory in Haryana is fantastic. These are centers of excellence that have done great work in these areas, and there is no limit to the kind of challenges that they can take on.

Another participant addressed a question to Sandhu. India has a long coastline, and there are a number of chemical facilities along the coast that are vulnerable to terrorist attacks. There are also 21 different ministries that coordinate security within India. Is there any hope of creating a Department of Homeland Security, as was created in the United States after the September 11, 2001, terrorist attacks? Is there any move to bring a coordinated approach toward counterterrorism?

Sandhu stated that there are 17 agencies that are involved in coastal security apart from the government of India itself. There are three different elements to the response that the Indian government has mounted, particularly after the 1993 Bombay attacks. There is the marine police. Every state is to have marine police stations. There is the coast guard, and then there is the navy. The traditional breakdown of jurisdictions has been by the number of nautical miles from the coastline. At a distance of up to 5 nautical miles into the sea, marine police are to address every incident. Between 5 and 12 nautical miles, the coast guard has jurisdiction, and beyond 12 nautical miles, the navy has jurisdiction over

response. There has been inadequate collaboration among these three organizations, and the marine police have taken a long time to develop. The people recruited into the marine police do not have sea legs, and they do not understand what operating in the sea water means. Sandu said that they have something called the National Committee for Strengthening Maritime and Coastal Security, and under that committee, a Maritime Domain Awareness Project is being pursued. The lead in that effort is provided by the navy, with the coast guard and marine police included.

The entire plan is yet to unfold, but it is in the process of being developed. Workshop participants may be aware that fishing communities are being contacted, and campaigns are being conducted among them. Selected fishermen are being given mobile phones and asked to report unusual events from the high seas.

All of that is being aggregated into a system. There are periodic exercises involving the maritime police, the coast guard, and the navy. The third layer remains weak. The navy and the coast guard are proceeding as they should, but the marine police are not yet as effective as they should be.

Another question was asked of Sandhu: Is there any indication that terrorists are resorting to newer, cheaper technologies for their attacks? If so, is there any way of countering this?

Sandhu responded that this is happening in two ways. About 8 years ago, India seized what was called a Radio-Controlled Aerial Module (RCAM) that had a wide span of about 6.5 feet and a capacity to carry about 3 or 4 kilograms with its own magnetic drop mechanism. The fact that terrorists had thought of this 8 years ago, and India actually seized RCAMs, which could be controlled from the ground, indicates that they have explored these options quite intently.

The second issue came up during the run-up to the Commonwealth Games in Delhi. There were a number of alerts about terrorists wanting to use micro lights. The difference between an unmanned aerial vehicle and the micro light is that the micro light must be manned. The advantage of the micro light is that noise levels are very low. It would not be detected as something unusual. Police had to undertake a number of measures to prevent that kind of activity as it is certainly within the realm of terrorist thinking.

The next question addressed social media. In the United States, offices are opening that are dedicated to social media and to obtaining useful information and getting it out to the public as well as to inhibiting misinformation. Is there any similar activity in India? How is social media being addressed?

Sandhu replied that he suspected that the participant was referring to using social media for propagating a viewpoint that a person believes is correct so that people can understand that perspective. Some of the better police forces are already doing this. The problem is how to detect the dominant sentiments, and which populations are affected by them? Once this is done, then we can create operational responses for mitigating misrepresentation that causes concern to people.

There are a couple of very interesting studies on this, including one by a company called Autonomy, which was bought by Hewlett Packard. They did a great job during the London Olympics, not just in mapping sentiments and identifying what was troubling whom, but also in judging peoples' reaction to the way in which the police acted in certain situations in order to provide scope for modifying their responses. There is a very interesting four-page paper available on the Internet with regard to Autonomy's success. There were 3 billion messages examined every day, which was interesting.

Following this, **Srinivas Mukkamala** stated that Sandhu had raised very good points regarding IEDs and tracking terrorist activities on social media. In the United States, universities are given problems to solve. One example was on a project called Computational Analysis of Cyber-Terrorism Against the United States.[8] Under this project, researchers were not allowed to examine what was happening in the United States due to privacy issues. Instead, they looked at Iraq, Afghanistan, eastern Europe, and several other countries. They were able to translate foreign language transmissions. Their examinatiton helped identify where people were buying raw materials, who was building what, and who was funding what, and they built a prototype and gave it back to the intelligence community where it can be used in models.

One of the aspects involved was investigating social media as a means of recruiting. This was very successful. They were able to build volumes of data to show how groups selected school students. They showed how these groups were infiltrating the U.S. school system, compromising websites, and posting positive messages about Islam.

Mukkamala came back to how scientific communities can help. There are several universities in the United States that were given really hard problems. While the suspect is working, the problem is also being explored by researchers to identify solutions and determine where basic research converges with operational issues. There was a project for the U.S. government on future combat systems that aimed to determine if it is possible to disable a future war fighter using radio frequency identification (RFID). They took an RFID tag, put a real mallet on it, and were able to disable the authentication between command control and a war fighter. This technology could take down pacemakers and insulin pumps eventually.

In the United States, SWAT teams assist cities, banks, and hospitals in identifying measures to secure their information. It has been working very well, and is a true private/public partnership where universities are given an opportunity to solve problems and still commercialize the solutions. Is there anything like this in India?

Sandhu replied that the Technology Based Incubator of Delhi University is one example. There is another initiative that has just begun at IIT Bombay,

[8]See Washingtonwatch.com. Computational Analysis of Cyber-Terrorism against the United States. Description available at: http://washingtonwatch.com/bills/show/ED_40857.html; accessed September 26, 2014.

called the National Center for Internal Security. IIT Madras is going to do some of these projects as well. There is a Reliance Institute of Communication in Ahmedabad, which is doing some work in this area. There are a number of enterprises, but Sandhu does not believe they have an aggregate view of what is happening.

Stephen Cohen asked what really inhibits the Indian government from being more proactive in terms of monitoring or attacking groups on the Internet?

Sandhu replied that this is a question of technical capacity, not a question of authority. Once they know how to do this, they can approach the government for authorization, and sections of the IT Act have relevant provisions. The government will not permit "fishing," i.e., the examination of a mass of information in a bid to find a needle in the haystack. The government will certainly permit directed monitoring. For that, they need to know the source of the trouble, which is where the scientific community can help. They can localize the target area.

Byron Gardner asked a question about the threats India is facing. He and his colleagues spent a great deal of effort worrying about attacks on distribution and transmission systems, transportation systems for liquid fuels, and public transportation systems. What is India's experience with attacks on those facilities and that kind of infrastructure?

Sandhu replied that as far as transmission systems and power distribution systems are concerned, they have had two kinds of attacks. The most frequent and most primitive has been to put explosives onto the feet of pylons and bring them down and thereby disrupt transmission. They have had to deal with any number of cases and in any number of states with that kind of activity.

This is not to say that people have not had their share of sophisticated attacks. They have targeted load dispatch centers, regional load centers, SCADA systems, and so forth. That is why the power sector has been one of the first to establish Computer Emergency Response Teams and Information Sharing and Analysis Centers. They are the ones that are networked with the national center; this is an ongoing effort.

As far as transportation security is concerned, Indian efforts have been more on the side of passenger security on metros and on urban trains. A number of efforts have been put into place to ensure security of those systems, but beyond this, not much work has been conducted.

2

Systems Approaches to Countering Terrorism

R. Narasimha opened the session on a systems approach to countering terrorism by stating that he was very glad to see that a meeting concerning counterterrorism was taking place, almost exactly 10 years after the first workshop on the same topic was held in Goa, India, in 2004.

SYSTEMS APPROACHES TO COUNTERING TERRORISM

Norman Augustine opened by saying that, unfortunately, the subject that brought this group of experts together is not pleasant, but it is of the utmost importance to both India and the United States. The interactions of the planning committees to prepare for this gathering made clear that the United States and India have a large number of common interests when it comes to countering terrorism, not to mention the fact that these two countries have both suffered greatly at the hands of terrorists. America has a great deal to learn from India's experience, he said, and he hoped that America's experience might prove of value to colleagues from India.

In the years just prior to the September 11, 2001 (9/11), attacks on the United States, Augustine served on a commission that was established by the U.S. Congress to investigate U.S. national security in the decades ahead. Arguably, the most significant sentence in the final report of that commission, issued a little less than a year before 9/11, read as follows: "terrorists and other disaffected groups will acquire weapons of mass destruction and mass disruption, and some will use them. Americans will likely die on American soil, possibly in very large numbers."[1]

The report proved, unfortunately, only too prescient when the events of 9/11 occurred shortly after the report was issued. One of the major recommendations of the report, which became known as the Hart-Rudman Report after the

[1]U.S. Commission on National Security/21st Century. *New World Coming: American Security in the 21st Century*. Washington, D.C.: Government Printing Office, September 15, 1999, p. 138. Available at http://gov.info.library.unt.edu/nssg/NWR_A.pdf; accessed September 15, 2014.

commission's chairmen, was to bring together the 22 different elements of our federal government that had significant responsibilities for counterterrorism.[2] When dealing with systems problems, such as terrorism, a fragmentation of effort is one of the greatest barriers to successfully carrying out the counterterrorism mission. Indeed, as experts in the United States belatedly learned following the events of 9/11, there had been warnings that, had they been able to fit the pieces of the puzzle together, might have helped avoid that tragedy.

The U.S. Department of Homeland Security (DHS) was created as had been recommended, but only after 9/11.[3] The scales of terrorism seemed to be tipped very much in the favor of terrorists. Terrorists can decide where they wish to act, when they wish to act, and how they wish to act. This places counterterrorist forces in the untenable position of having to be prepared for everything, everywhere, all of the time; something that is an obvious impossibility.

The terrorists' range of choices extends all the way from biological attacks to physical attacks, from attacks on the economy to attacks on the food supply, and far more. The implication seems that the defense has to be prepared to take an offensive role as well as a defensive role, something that could be very controversial. This, along with other possible actions, requires balancing risks and intelligently allocating resources. That, of course, is "systems thinking."

Augustine continued his introductory remarks about systems thinking as it relates to the counterterrorism mission and set the stage for other, more specific examples, and case studies that followed throughout the workshop. He explained that the deterrence strategy of the Cold War is now rather bankrupt when one deals with terrorists. It assumes a rational enemy, and, in particular, an enemy that does not wish to die in carrying out its aims.[4]

In contrast, many terrorists are willing or even desire to die when carrying out their activities on behalf of their cause. We have seen this both in the Mumbai attacks and on 9/11. Augustine argued that in the intervening years since the Cold War ended, two major changes, both brought about by technology, have profoundly affected the role and consequences of terrorism. The first of those changes was what we have come to call globalization. The second is the amplification of destructive power available to individuals.

With respect to the former, modern jet aircraft have made it possible to move things, including people, around the world at very nearly the speed of sound. Modern information systems have made it possible to move ideas, knowledge, and data around the world literally at the speed of light. Frances Cairncross referred to this phenomenon as the "Death of Distance."[5] Indeed, distance has died. What

[2]U.S. Commission on National Security. *New World Coming.*

[3]U.S. Commission on National Security. *New World Coming.*

[4]Some experts caution that not all those who study terrorists agree that Cold War deterrence should be applied to the terrorist challenge.

[5]Cairncross, F. *The Death of Distance: How the Communications Revolution Is Changing Our Lives*. Boston: Harvard Business School Press, 1997.

happens in Bangalore now matters in Boston. What happens in New York now matters in New Delhi.

Then turning to the magnified power of the individual, Augustine stated that for the first time in the history of the world, individuals or very small groups acting alone can profoundly impact the lives of very large groups of people. That is a big change. This has been the consequence of nuclear weapons, biological weapons, and to a lesser degree, radiological and chemical weapons, and other kinds of attacks. These developments have been exacerbated by the growing interconnectivity and interdependence across nations and within nations of supporting assets as well as the concentration of people in small physical areas.

Terrorists who seek to exert the use of some weapons cannot maintain control over the people that they attack, but they can fairly well deny effective control over their population. Certainly, it makes no sense for terrorists to engage in conventional warfare with powerful nations like India or the United States. That is why, of course, they become terrorists. The impact of such individuals and groups can often produce a psychologically disproportionate effect on the populous.

This is where the amplification factor takes place. An example with which Augustine is intimately familiar and concerns two young men, not very bright young men, who had one weapon, namely a rifle. A few years ago, they terrorized Washington, D.C., for more than a week. They created traffic congestion throughout the metropolitan area. They succeeded in killing 10 innocent people, but that was during a time period when 10 people died in our same area due to automobile accidents that went largely unnoticed, other than by their families and friends. There is an amplification factor that makes smaller acts have a powerful impact.

So what is to be done? Augustine argued that to begin, terrorism does have to be viewed as a systems problem. By that, he meant that the challenge of terrorism has to be addressed in its whole, not individually by addressing only parts of the problem. This permits one to optimize the use of one's resources and to look for weak links in the chain that often can reveal very highly leveraged actions that the counterterrorist forces could take.

Consider the possibility of using commercial aircraft as a weapon, as happened on 9/11. That was something that had certainly been addressed well before 9/11 by security organizations, and, unfortunately, by terrorists as well. Examining this possibility as a systems problem requires an examination of all of the elements involved. One might have concluded that the best option one could take would be to reinforce the cockpit doors on commercial aircraft. This is not a high-tech solution and not a very expensive solution, but had that been done we probably could have prevented the 9/11 attacks from occurring, at least the way in which they occurred.

The challenge, of course, is that systems problems tend to be exceedingly complex, terrorism being one of the ultimate examples. Consider, for example, the simplest of all possible systems, a system that has two elements that can impact each other in a binary fashion, either on or off. If one has two elements,

obviously there are four possible states for that system. One could have each element impacting the other, neither impacting the other, or the first impacting the second, or the second impacting the first. There are four possible states for the system with just two elements.

If one advances to a system with three elements, one discovers that there are suddenly 64 possible states. Professor Frederic Whitehurst of the Max Planck Institute derived the equation that describes a number of possible states for a complex system. He appropriately called his equation the "monster." Indeed, it is a monster. If there are just seven elements in a system of the type described, the number of possible states exceeds the number of stars in our galaxy. The conclusion is evident. One cannot plan for or even consider every possible situation in a complex system. That underscores the importance in systems thinking and systems engineering of risk management, and of trade-offs. One cannot do everything. Systems thinking could help reveal how best to allocate limited resources.

To answer questions like these, one first must learn to think like a terrorist, something that is not easily done. Second, one has to understand one's own value system and the terrorists' view of that value system. When dealing with threats that are both likely and highly consequential, one is generally best served by a defense-in-depth approach because no single layer of defense is likely to provide a sufficiently high degree of protection.

Fortunately, the challenge of a complex system applies to the terrorist as well, which is why one can maintain hope for the defense. A simple example would be to have a magnetometer in one area of an airport and have a chemical sniffer in another area and another area would have dogs. Then these areas should change from time to time so that an attacker could not be aware in advance of what sort of sensing would be in use at any given time.

Furthermore, a strategy of this type requires the attacker to be better coordinated. Even if the individual elements are not terribly effective, they may force the attacker into a situation where he or she is vulnerable to other means of detection because of the need for more coordination and communication. Augustine cited an example of a non-high-tech case that occurred during the Vietnam War when a U.S. artillery base was continually under attack in the middle of the night by Vietcong. The commander did a systems analysis of the attacks.

It occurred to him and to his colleagues that the enemy had very poor tactical communications. They had to plan the attacks in advance, rehearse them, and coordinated them well. It occurred to him if he could get inside of their communications cycle, he could change the entire situation. First, they put all of the guard towers in the defensive positions on skids. Every evening just before dark they would take bulldozers out and move them all around and change the puzzle, and they were never attacked again at that particular base. It is a very non-high-tech example, but a very effective one, resulting from systems thinking.

Augustine returned to the subject of defense in depth and not being confined to a purely defensive posture. It is important to understand the enemies'

motives, and their limitations. The latter is a very great challenge in democracies and free societies. It is very likely that this will become a greater and greater issue as technology advances further. The question is how does a government protect its citizenry against terrorist attacks, and at the same time not invade the privacy that those citizens expect living in a democracy.

Given the understanding of values that one assigns to one's own assets, both physical and societal, and an understanding of the enemy and the enemy's modus operandi, a systems approach would call for disrupting potential attackers' plans through both active or passive means before they could take any action, as well as taking actions to minimize the impact of an attack, should it occur. Having done a defense-in-depth analysis, what remains is to enhance the defenses of important targets, to counter whatever attack actually occurs, and finally to recover from the attack. An important aspect that is rarely discussed is being able to provide forensics analysis that can point to the origin of the attack.

It is noteworthy that an informed citizenry could do a great deal to help protect itself. However, Augustine's own admittedly nonscientific surveys in the United States reveal that most citizens, even generally well-informed citizens, are not aware of what they can do to help protect themselves. For example, if one goes out on the street and asks people what they should do if there is a chemical attack, go to the attic or the basement, or if one asks, in the case of a nuclear attack, should one go to the basement or to the attic, most people do not know. In the case of a radiological attack in a particular area, should one try to go to the north, to the east, to the south or to the west, depending on the prevailing winds and the given locale? In the case of a biological attack, should one go to the hospital to get a vaccination or should one stay at home? If one stays in the house and seals the doors and windows, how long could one live before becoming asphyxiated? Augustine's surveys show that very few people know the answer to any of those questions. Yet, were they to know, they would be able to greatly reduce the casualties in the event of major attacks.

Finally, he noted first and foremost, when dealing with both terrorism and counterterrorism, one is dealing with people. In addition to cases where people unintentionally fail to carry out their responsibilities, there are cases where people can intentionally cause harm or fail to carry out their responsibilities. The latter are cases of insider threats. This could be forestalled to some degree through thorough personnel assessments, through random task assignments of personnel, and again through defense-in-depth, including the use of so-called two-key control systems. Understandably, human behavior does play an important role in both the success of terrorists and the success of those seeking to counter terrorism.

Augustine recently had the occasion to investigate, on behalf of the U.S. government, an incident that occurred at the Y-12 nuclear facility in Oak Ridge, Tennessee, during which an 82-year-old nun and two 60-year-old drifters cut through four secure fences and went through three secure zones in the middle of the night at one of the United States' most highly defended facilities without being detected. Presumably, they were not terrorists. They were protestors. They

reached the outside of the building that was being protected. No one arrived to arrest them.

This was all recorded on night vision television. They took a hammer out of their backpack and proceeded to pound on the walls, hoping to bring a guard to arrest them. The guards heard the pounding and thought the carpenters were working late that night. Ultimately, the intruders were arrested. One has to ask: How could this possibly happen and could this happen anywhere else? There were many factors that contributed to this incident. However, these factors could be summarized in one word: culture.

First, the guards, in many cases, went to work every day knowing that it was highly unlikely that in their entire lifetime they would ever face a real threat. Second, in this case, the electronic warning devices had so many false alarms that the guards generally did not pay much attention to them. Third, realistic training exercises were not possible because if they were sufficiently realistic, people would be killed. Added to this, the guards' responsibilities at such facilities are immense.

In other words, guard positions require intelligent people. There is nothing more boring than standing in a dark hallway holding a rifle for 10 hours a day. These are very bright people in a very boring job. That is a hyperbolic combination, to borrow a phrase from aerospace. Based on this incident, it was concluded that one has to rotate work assignments, work shorter shifts, certainly demand higher levels of discipline, and conduct every possible form of training that remains safe. One cannot reduce risk to zero, however.

By examining terrorism as a systems problem, it would appear that by prioritizing vulnerabilities, the value of assets, and the choices one has, the impact of terrorists could be substantially reduced. Augustine suspects that taking this systems approach has been one of the factors that contributed to the reduction of terrorism in both the United States and India in recent years. The same can be said for successful acts of terrorism: thinking systematically has produced many deadly acts of terrorism. That is something Augustine never would have predicted on 9/11.

Augustine concluded by saying that he hoped his remarks would be useful. He expressed his expectation that he would learn a great deal from Indian colleagues and from American colleagues. He expressed the desire to contribute wherever he could, because this gathering could make a great difference.

INDIAN RESPONSE REGARDING A SYSTEMS APPROACH TO COUNTERING TERRORISM

Nehchal Sandhu said that the government of India recognizes the value of all of the propositions Augustine raised. They realize that a systems approach is the only way to deal with this very complex problem, and they have their own experiences with regard to employing a systems approach.

Sandhu stated that the need for a systems approach was first recognized in the late 1990s during the Kargil episode. A large number of regulars and irregulars of the Pakistani Army entered the Indian side of the Line of Control in a part of Jammu and Kashmir, and remained there for some time until they were evicted. There was a Kargil Review Committee, and then a group of ministers read the recommendations that flowed out of the four task forces that were established. One of the main recommendations was that India needed to have a MultiAgency Center, which meant that all of the agencies involved in security, in collecting intelligence, and in implementing preventative plans should be able to get together. This was not just to make them collectively aware of what the threats are at a particular juncture but also of how to formulate response strategies so that the threats could be mitigated and addressed. The MultiAgency Center opened in 2001, and started with 14 or 15 agencies. Cultural inhibitions prevented participating agencies from sharing everything necessary. As result, the MultiAgency Center did not progress as well as it should have. The Mumbai attacks are an example of handicaps in India before the MultiAgency Center became effective.

There was intelligence about a possible attack through a vessel coming in across the west coast. There was intelligence to suggest that these people had taken off from Pakistan. The precise landing point and other details were not known. The Minister of Home Affairs, who is now the finance minister, P. Chidambaram, took it upon himself to breathe new life into the MultiAgency Center. He issued a new order at the end of December, creating a new means of collaborating within the MultiAgency Center. He did not opt for the creation of a crowning hierarchy in something like the U.S. DHS, because he believed that it would be difficult to aggregate under one leader. He thought that whatever is worth focusing on could be brought to the table before the agencies that were concerned.

Today, India's MultiAgency Center has approximately 26 or 27 agencies, right across the board from Revenue to Intelligence to Response Mechanisms, and so on. They meet every day at 3:00 p.m. Every one brings to the table anything they may be aware of with respect to developing threats. A discussion is held. Responsibilities are assigned for any developing leads. The next day, all the collected information is reviewed in addition to reviewing new intelligence.

Interestingly, one of the subsystems introduced into this mechanism was the concept of focus groups. Not all 26 or 27 agencies need to be involved if the issue is not relevant to their expertise. For example, if the issue is not something associated with finances or movement of terrorist funding, the Indian Revenue Service need not be burdened with participation in those focus groups dealing with other issues. The issue is taken to the people who have provided the intelligence, those who can supplement it or create corollaries and substantiate or enrich the intelligence. Another group consists of people who are actually responsible for responding to the intelligence. These focus groups then have continuous meetings, and they work on the issue until the problem has been resolved.

Therefore, today there is a platform where all of the relevant agencies participate. Each maintains its identity, but everyone sees everything. Those that need to act have a mandate and a responsibility to do so. The founder of the center did not want to create Standard Operating Procedures for every kind of contingency because that would have introduced rigidities. Incident commanders are free to develop their own approaches.

Within this entire system of dealing with terrorism, as Augustine mentioned, the government of India has taken note of the role that the public can play in warding off terrorist threats through sheer observation of what is occurring on the ground. There are sensitization programs undertaken by every police officer with communities to enlist their cooperation and to be able to provide a better response.

The government is also installing a number of closed-circuit television cameras in big cities. Mumbai will have 6,800 cameras once they are all installed. The cameras will have very sophisticated regional and centralized analysis centers, which would then aid response forces dealing with these types of situations.

Sandhu also noted that in India potential terrorist targets are protected by first identifying the people who might be attacked. Threat assessments are conducted by all of the relevant agencies. Then a designated group determines what type of protective security needs to be provided to each individual.

With regard to facilities, India has three types of installations, A, B, and C categories. Every facility is first inspected, and then a menu of necessary security equipment is purchased for them, and they are required to comply with these purchases. In A-category facilities, an annual review is conducted and people who have access to sector-relevant intelligence go to the facility and determine whether the facility is in compliance and whether they need to adjust any part of the defense system to ensure that new threats are considered and addressed. B-category facilities are inspected once every two years, and C-category facilities are inspected once every 3 years. The door is always open for discussion to every facility director to address any new concerns if a matter has emerged in that neighborhood.

Two kinds of counter-terrorism capacities have also been developed. One requires every state to establish an anti-terror squad and special task forces. These groups have a dual role. They have a role in responding in the event of a terrorist attack. They also have a role in investigating terrorist cases. If the crime scene is not preserved, then a lot is lost right away. If the first responder is the person who has to investigate subsequently, he or she will hopefully make certain that the crime scene is protected and that the necessary experts can then come in and recover available forensic evidence available.

Sandhu added that they also increased their capacity for forensic analysis. They are now able to determine on the basis of very small, pico-quantities whether a certain explosive was used or not used, what kind of detonators were deployed, and what kind of timers were employed. That all feeds into the second part of the response, which for a complex incident or a multi-scene event, is

coordinated by the National Investigation Agency (NIA). This is a new, specialized agency that came into being about 5 years ago to only deal with terrorist crimes. Unfortunately, in the Indian legal environment and federal structure, law and order and crime investigations are handled by provincial police offices; therefore, the NIA does not investigate terrorist cases unless invited to do so.

Normally, the state response mechanism, which could be the local anti-terror squad, does the basic response work. They preserve the evidence and the NIA works alongside the local group, but is not in the lead. Only when notification is issued by the government is the investigation transferred to the NIA.

India also has the National Disaster Management Authority (NDMA) that can be deployed if biological agents, chemical agents, nuclear agents, or any material of that sort affecting large sections of the community are used. NDMA has a response capacity, including trained personnel and materials that they can move to affected areas, distribute, and use to prevent loss of human life.

DISCUSSION

To open the discussion, a workshop participant noted Augustine's comments about the Y-12 incident. A month prior to the incident, there was an international training course on physical security at the facility. However, when there is training and then something like this happens a month later, the training does not seem to have been adequately effective. How can training be more effective?

Augustine agreed that this is a profound question to which he wished he had an answer. This was a case where the challenge was recognized, and for a variety of reasons they never were able to focus on the issues cited, and they paid a price for it.

Augustine returned to Sandhu's comment on the recommendation that 22 organizations should be compiled. The point was made that this is difficult because one has to be careful not to create a super-bureaucratic organization without creative, imaginative, fast-on-your feet people. Just as an interesting case study, when the United States created DHS, Augustine was on the President's Homeland Security Advisory Council. He spent a good deal of time trying to help the U.S. government determine how to organize DHS. By coincidence, at the same time Augustine's corporation was in the process of acquiring 22 different companies, the same number of the elements of DHS. The corporation had almost exactly the same total budget as DHS, which at the time was $45 billion per year. They had the same number of employees, which was about 185,000 people.[6] Within a year from the time the corporation merged those 22 organizations together, they truly operated as one organization. DHS, as good as it is, is still struggling, in Augustine's opinion, to act as one entity. As he has learned

[6]Department of Homeland Security. "Budget-in-Brief Fiscal Year 2014." Available at http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20(4).pdf; accessed October 16, 2014.

from spending 10 years in government, it is just a lot harder in a democracy to make things happen than it is in the private sector, where people who do not "get with the program" go somewhere else. It is just a common challenge.

S. Chandrashekar asked: If there was a terrorist attack in the United States and there was a local response, what would be the role of the security structure? What would be the role of the state structure? Who has the final authority in the United States? What is the state-level coordination mechanism in India? How effective is it? Are there jurisdictional or turf-related issues? Is there a better way to clarify this authority?

Sandhu replied that the Indian constitution outlines a certain distribution of responsibilities, and not until it is amended, and that is unlikely to happen, will it be possible to rebalance and reapportion the authority of the provinces vis-à-vis the central government. The reality of the situation is that if a terrorist strike were to occur, the administration or the jurisdiction affected would be very interested in cleaning the area and trying to successfully detect and prosecute the perpetrators. They therefore would work very hard. Also, if they fairly quickly discern that they are not able to make headway, then they would request central support and the NIA would assist. There is little resistance to requesting central support, which would entail flying in forensic teams, bomb disposal experts, and even expert investigators. For the most part, provincial jurisdictions are quite happy to receive additional assistance from the central government.

Augustine provided a similar example. One of the successes accomplished in the United States since the events of 9/11 is that there is a very clear, agreed-upon protocol of who is responsible for what. To oversimplify, the initial tactical response is left to the local organizations. If the events become greater than they are able to deal with, the federal government comes in and helps. Even in the former case, the federal government has much better forensic capabilities, for example, so the local governments can and do ask for support. There is a point at which authority transitions, depending on the nature of the attack, but it clearly starts with the local authorities and the first responders.

Another workshop participant then added to Sandhu's statement. The participant had the opportunity to work with the weapons of mass destruction (WMD) unit of the Federal Bureau of Investigation (FBI), which had five or six members. They clearly stated that when any incident of food terrorism occurs, state officials immediately contact this unit. For food safety issues, the local and state police address the issue, but if the incident escalates, the FBI or federal police are called.

Augustine added that there is another interesting aspect to security. Approximately 90 percent of the assets that are to be protected in the United States do not belong to the government. They belong to the private sector. We are not as good as we need to be in incorporating the private sector. There certainly has been work done in that area through industrial associations and through contacts with individual organizations. For example, U.S. power systems, food supply, rail transportation, air transportation, and any number of other critical elements are principally in the private sector.

Following up on the issue of federal and state coordination, **Stephen Cohen** suggested that it would be useful to compile case studies or examples and compare the two countries' experiences. There is obviously going to be cooperation in the event of a crisis. It may be helpful to systematically examine how this cooperation adapts based on lessons learned regarding prosecution, preparing for future events and immediate response. This may be an area for larger collaborative work involving social scientists and perhaps historians.

John Holmes supported Augustine's comments as one who had served as a federal responder and then became a local responder. The blueprint that the United States uses is the National Incident Management System (NIMS), which is available through the Federal Emergency Management Agency. It is exactly as Augustine described. Depending on the complexity of the events, response may begin very locally and then grow much bigger and bring in the federal government.

NIMS is a system that is designed to be very flexible as response grows to bring in other agencies with other capabilities. NIMS was developed locally in California, was adopted by the U.S. government, and has been the template that has been used for many, many years in responding to all kinds of incidents. It could respond to a WMD event although it was actually developed to respond to brush fires in California. Having a blueprint to bring everyone together to work on dealing with an incident is a flexible way of being very inclusive of all agencies. In Holmes's experience working at the Port of Los Angeles, this system was used many times when an incident occurred and the initial response was by a local law enforcement agency and then subsequently, local officials called in customs officials, the FBI, and many of the other agencies to work cooperatively.

At the end of the day, the blueprint allows for joint handling of constituent groups and joint press releases. Everyone wants to respond to the event when an event occurs, but one also has to be able to deal with other externalities that are sometimes quite difficult, such as dealing with labor organizations and the media.

Referring to assets in the private sector, **Srinivas Mukkamala** stated again that 90 percent of structures and systems in need of security in the United States are owned by the private entities. This makes responding to a cyberincident rather interesting. For example, there are relatively few hospitals dedicated to treating the most critical trauma patients. These essential hospitals are vulnerable to cyberattacks that could deactivate electrocardiogram machines, electroencephalography machines, endoscopes, and ventilators. Recently such an incident occurred at a trauma hospital. Local and state law enforcement agencies do not have the capability to detect or thwart cyberattacks. In the case of the trauma hospital, private forensics investigators were brought in. The state police observed and coordinated with the Justice Department. Rather than making it a cyber law enforcement incident, responders wanted to contain the attack first. They contained the attack in the same way one would address an attack on a

civilian facility. Once they were able to bring the hospital back online within 24 hours, law enforcement responses began.

Many responses work in a cohesive way rather than running into restrictions. They try to contain the attack first and then determine the proper jurisdiction. If it is a multistate incident, the FBI has jurisdiction. The incident described involved multiple countries; therefore, the Justice Department involved several other counterterrorist specialists to determine if the incident was one of terrorism or if it was a different type of attack from a particular country. More than seven departments worked together on this incident, and this is occurring more and more frequently, especially during cyberattacks. In the United States, there are several FBI field offices that have the capability to be called in to help immediately.

David Franz noted that Augustine mentioned the importance of culture in the systems approach to dealing with terrorism. Culture, Franz believes, is defined by humans with leadership skills and with technical depth. Having expertise in many areas is important in dealing with terrorism because there are so many unknowns. One cannot plan for a specific kind of a problem.

In the world in which Franz grew up, which was the military, medical, biological defense world, the environment went from the Cold War, in which there was deep technical expertise, to a model where the United States is running people through the system and checking boxes and making sure they had some experience, but not leading. The system was trying to promote staff, but not leaving them in place long enough to become experts. How is this system working in India, and has a solution been found to ensure that the right young people will have expertise and leadership skills? A participant from India replied that this is an area where they are still challenged. They have not been able to overcome the cultural obstacles to create a uniformly acceptable plan of action.

In reply to **Micah Lowenthal's** request that Augustine share some of the mistakes that were made in DHS that inhibited the systems approach, Augustine said that he should probably preface his remarks by saying that, overall, he thinks the creation of DHS was the right thing to do and is being carried out very well. There are clear short-comings. The principle short-coming in his mind is having several independent "stovepipes" (separate hierarchies of authority, responsibility, and communication that do not interact). Today, there is one organization with many independent stovepipes, and those stovepipes have to be broken down. That requires strong leadership at the top and strong support at the bottom, neither of which are always easy to come by. This will happen, but it is taking a lot longer than Augustine thinks it should have.

Also, he believes that DHS is not as advanced as he had hoped they would be in technology areas. The original plans included a strong technology effort within or at least funded by DHS. That technology effort has never grown to the degree that many in the United States had hoped it would, partly due to a cultural issue associated with the fact that most of the entities that made up DHS were not high-tech organizations. The leadership was made up of people who general-

ly did not have strong technology backgrounds, although there are exceptions. Funding is also an issue. That particular effort was just not funded.

Rita Guenther then asked a question first of Sandhu: Who might comprise the review committees mentioned in his earlier remarks, and how is the scientific expertise for those review committees sought, when the area or the topic permits it or would benefit from it? She then asked a question of Augustine. As someone who has a very broad and diverse set of experiences, how should one go about organizing the thought process to start a systems approach? In other words, how should one begin the thinking before one actually can implement a systems approach? Is there a set of questions that one should ask? How does one even start to think about developing that systems approach?

Sandhu replied that the review committee he referred to deals with the issue of monitoring of communications. It might astound the audience that India depends on legislation from 1885 to conduct monitoring. It is called the Indian Telegraph Act. The second and supplementary legislation that aids in this area, particularly for data, the Information Technology Act, was adopted in 2000.

The Indian Telegraph Act of 1885, Section (2) gives the government the authority to monitor communications. It has been under review several times and it has been challenged often. The most detailed and critical judgment came out of the Supreme Court in 1999. First, it upheld the authority available to the government under the Telegraph Act to carry out monitoring in specific cases. Second, it laid out guidelines as to how these authorities are to be exercised. Third, the court insisted on a better review mechanism. The government had to do all of this. Then they went back to the Supreme Court for their determination of whether or not what they had put in place was satisfactory. With reference to the approvals, first, if there is anything within the government that needs monitoring, there are only seven or eight authorized agencies that can do it. They have to present the reasons for the request within the institution. The head of the institution has to be satisfied that the request is actually justified. He or she will then approach the union home secretary. That is like the federal person in charge of internal security. The home secretary's office will examine the request and decide whether to accept it or not. It is worth noting that all requests have to relate to a specific entity. One cannot just draw buckets of traffic out; the request has to be in reference to an entity. A decision is then taken. It is interesting to note that 20 percent of the requests made are rejected.

If a request is approved, every month thereafter a review committee meets, including the Cabinet Secretary, the top-most official of the government of India supported by the law secretary that looks after the legal affairs within the government of India, and the Department of Telecommunications secretary, who is not a part of the authorization process, but whose department facilitates the implementation of the authorization of the Home Secretary. They look at these orders and decide which ones can be allowed to remain in effect and which have to be withdrawn. There, again, there is a 5 percent rate at the end of the review committee.

Orders are usually valid for 60 days, and the review committee meets well within that. If the committee judges any particular activity to be inappropriate, it is terminated, and everything related to that activity has to be destroyed right away. That is how it works. Incidentally, this process of the review committee was taken back to the Supreme Court. They were asked to satisfy themselves as to whether this was adequate, and they approved it. Ever since, it has continued as such. We have had many interventions by enthusiastic lawyers who still wish to question the methods in place. The Supreme Court has again come back and said this process was sufficient.

Augustine responded to the question about how one would go about creating a systems capability, for example, within DHS or within the government as a whole. Unfortunately, traditional organization charts do not lend themselves well to taking a systems approach. The reason for this is that organizations tend to be broken up into entities that carry out a given function or given mission, which makes a lot of sense. It does not lend itself well to making trade-offs between the various elements of the organization.

Augustine believes that what is needed is a very small group at the very top with the overall assignment to prevent terrorism. That is simple in statement, but not simple in execution. That group should have the overview to address any issue that relates to terrorism and its impact. Years ago, he served at the U.S. Department of Defense (DOD), which, at that time, was certainly stove-piped. There were very few trade-offs made. Then during the Cold War they created a small group made up of perhaps 20 very imaginative people. They were given the task of being creative and innovative and to do an analysis of the trade-offs. They made trade-offs between civil defense and the number of submarines. The first reaction was: How is that done? They never came up with a universal equation that let one do that, but they shed a lot of light on it. Basically it became an issue of how one invests resources to deal with this overall issue.

At the time, Augustine was in DOD and was always amazed that for many years a third of the budget went to the army, a third to the air force and a third to the navy. It is quite a coincidence that that should be the optimum way to spend the budget. He was not suggesting it was easy to get away from that, but movement was made. Budget allocations need to change from time to time depending on the circumstances. Augustine added that he is a strong believer that a systems group as he has described needs to have not only a strong intelligence input but also a strong red-team that can pretend to be the other side, or to be the bad guys and try to think like the opponents think. That is not usually done. That does not make it less important.

There is significant benefit to be gained from that approach and from bringing in independent, outside thinkers to challenge them. When he was involved with the army, there were some facilities that he was concerned about and the army assured him that they were absolutely secure. He went to the Air Force Special Forces and the Navy Seals and asked how secure the U.S. Army's facilities were. Of course, this became a great challenge to them. "We learned a lot of things that we would not have learned by asking our army." He did not

intend to demean the army in anyway, but one can become brain-locked, and that is what one has to avoid.

Another participant asked a question of Sandhu. There are systems approaches when developing a plan, and conducting research and development for defense activities, but when responding to a terrorist attack, following the systems approach can prove to be very lax, as occurred in the Mumbai terror attacks. It took 3 days to eliminate all of the terrorists. There must be a need to develop state forces for counterterrorism tasks. There must be some out-of-the-box thinking to respond quickly to such attacks.

Sandhu replied that he does not think it was a lack of a systems approach that detracted from the efficiency that needed to have been brought to bear on the Mumbai attacks. There are internal reviews that have brought forth facts, which are not in the public domain and which he was not free to discuss. No matter how good the system is, it will not be effective unless people are efficient.

With regard to the state police forces that need to have antiterrorism response capacity, first, the National Security Guard, which is the key response mechanism, now has four regional response hubs. Mumbai is one of the hubs, along with Calcutta, Bangalore, and New Delhi. That brings the response capacity closer to the possible areas of attack. India also has a new group created after the events in Mumbai: Force-1. This is a state-owned capacity to deal with terrorists in a tactical manner. It is something like a SWAT team with no component for investigation. Rather than create new forces, other states are going into the domain of reinforcing their antiterrorist squads, and their special task forces so that they have what is necessary to deal with a terrorist incident.

Cohen asked Sandhu to provide suggested readings on the Mumbai case. *The Siege,* by Canadian and French journalists, has received considerable attention in the United States.[7] Is there a better book? What, in the public domain, would be a useful guide?

Sandhu replied that the National Institute for Advanced Studies has done a great job inviting people to speak at this workshop about the Mumbai attacks. The joint commissioner of police in Mumbai is one of the people who was at one of the attack sites and actually fought the terrorists and was injured in the process. He is very familiar with what happened and how it happened. He has been associated with all aspects of the tactical response, the investigation, and the reviews that followed. There is also a report by R. D. Pradhan on the Mumbai attacks, which is available on the Internet.

A participant asked Augustine about how DHS was established, how leaders with strong technical backgrounds were identified, and what role they actually played in establishing DHS. Augustine replied that he was referring to the importance of having people with a strong technical background because so

[7]Scott-Clark, C. and A. Levy. *The Siege: 68 Hours Inside the Taj Hotel*. New York: Penguin Books, 2013.

many of the problems and so many of the solutions to the problems the world faces are technical. Certainly, terrorism is an example in many instances, but not all. Because it is important to have competent technical people in senior jobs where there is a lot of technology involved, Augustine wished he could say that they were successful in attracting a large number of technical people into the government to do this. Frankly, in his opinion they were not.

There are some technical people at relatively senior levels, but they are disproportionately few. For some reason, within the United States, it is fairly unusual for technical people to take senior positions in government. There is trivial representation by technical people in the U.S. Congress, and Augustine thinks that this is one of the concerns that the United States should have. This is partly the fault of technologists, such as himself, who do not want to be involved with politics. Many find it offensive, so it is hard to get them into government. It is not hard, however, to get them to criticize the government.

Another issue is that over the years, many conflict-of-interest rules have been created that have made it very hard for people to have a career both in government and outside of government. Augustine spent two tours in government, and that would not be possible under today's conflict-of-interest rules. Some would say that is good, and others would say maybe it is not.

Another participant asked about bioterrorism. Since the 2001 anthrax attacks, considerable focus globally has been given to the bioterrorist attacks and to biothreats emanating from national sources as well. However, there were relatively few casualties in the United States as a result of the anthrax attacks. Subsequently, in 2009, as a result of the swine flu pandemic, there was a large number of casualties all across the world. This raises the question of addressing the issue of biorisk management from two perspectives. One is from the security-centric perspective, and the other is from the public-health-centric perspective. Irrespective of the sources of this accidental or deliberate act, the consequences are almost similar. How would a systems approach address this to create a balance between these two, not entirely complimentary, but a little bit contradictory, perspectives to manage the biorisk? At the same time, this also involves a great deal of intersectoral cooperation between the security establishments and the public health professionals. How does a systems approach address these two issues?

Franz replied that this is a very important point. He has long said that we should have an all-hazards approach, and in the United States, the Centers for Disease Control and Prevention (CDC) should be the lead agency. This, again, is a cultural issue. Franz believes that CDC feels that there are more important issues to address than security issues, although they have become much more involved than they ever were. They were first funded for biosecurity activities in 1998. Before that, they had no funding for this type of work, but they did work with DOD to some degree. As long as there is one group waiting for a bioterrorism attack, which may be rare, and another group working with naturally occurring and emerging infectious diseases, which are quite common, the second group will be the most competent to deal with the bioterrorism attack. Franz

would use an all-hazards approach with the medics and CDC in the lead if he had the choice, and then add a few extra important capabilities that would be needed to respond to a terrorist attack. He believes, however, that the United States has looked at bioissues mainly as a security problem and has added some medical capabilities into the mix.

A participant followed up with a question about how to balance the security and technical aspects, especially in areas such as bioforensic investigations that require technical expertise. Is this also in the domain of law enforcement? How does one manage this balance?

Franz replied that he believes that the United States has been quite successful. Right after 9/11 and 10/04 (the anthrax letters), an FBI individual was placed with CDC teams as they did their epidemiological studies of naturally occurring outbreaks. This was a very positive and very useful step. Now there are FBI forensic experts who have an understanding of medical and infectious disease epidemiology, which they did not have before. This was fairly easily done. It would be better to have the medics in charge and add in the security expertise as needed, rather than have the security people responsible and add in the medics. As a medic, Franz admitted that medics do not always respond as they should in such cases, therefore, security training is also needed.

3

Protecting Critical Infrastructure

SECURITY AT CHEMICAL FACILITIES

John Holmes, session chair, opened by discussing the importance of providing security to critical infrastructure, in part because of the impact that infrastructure has on the economy. The Port of Los Angeles, where he was director of operations for 7 years, handles approximately 43 percent of all of the cargo coming into the United States.[1] If the port is shut down, the impact on the U.S. economy would be several million dollars per day.[2] Holmes and his colleagues are obviously very concerned about critical infrastructure security, including chemical facilities.

Securing Chemical Facilities: Recent American Experiences and Lessons Learned

Nancy Jackson provided context for her comments by stating that Sandia National Laboratory conducted the first post-September 11, 2001 (9/11) security assessment on the Los Angeles-Long Beach Port Complex. As a result of this experience, she spoke not only about the security of facilities, but also about keeping chemicals safe from being misdirected or stolen for use as explosives or in making illegal drugs. Methamphetamines and similar drugs are a significant problem in the United States. There is also concern about facilities being sabotaged, and the chemicals being used as weapons once the facility is compromised. The release of chemicals can cause all kinds of problems.

It is important to limit access to chemical facilities. Before the 9/11 attacks, this was not done very well. There were few, if any, security checks, or

[1]Congressional Budget Office. *The Economic Costs of Disruptions in Container Shipments*. March 29, 2006. Figure 1. Available at: http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/71xx/doc7106/03-29-container_shipments.pdf; accessed September 18, 2014.

[2]Capps, L. "Recognizing the 100th Anniversary Year of the Founding of the Port of Los Angles." In *Capitolwords*, vol. 153, no. 185, December 5, 2007. Available at: http://capitolwords.org/date/2007/12/05/H14212_recognizing-the-100th-anniversary-year-of-the-foun/; accessed September 20, 2014.

checks on personnel that worked in chemical factories. In Japan in 1995, Aum Shinrikyo was able to recruit several chemists to help them make sarin gas, which they released in the Tokyo subway.[3] In addition to the chemicals themselves, chemistry expertise and cybersecurity are important for ensuring safety and security at a facility. The latter is important at chemical facilities and large manufacturing sites because cyberattacks may be used to sabotage a plant.

Chemicals have a unique role in weapons of mass destruction. They are different from biological, radiological, or nuclear materials in several ways. There are chemicals everywhere, and many of them have dual uses. Isopropanol can be purchased at drug stores in the United States. It can be used to clean a wound or clean eye glasses. Isopropanol can also be used to make sarin. There is a lot of isopropanol currently being removed from Syria, for example.[4] Chemicals are also essential for an economy. Almost all products on the market today started from chemicals. The size of a country's chemical industry can often be a sign of the size of a country's economy. As a result of their importance, it is not possible to lock chemicals away as one can secure uranium or plutonium. Rather, chemicals management is required from cradle to grave, beginning to end. Management of the entire chemical life cycle is needed for security purposes, whether it is management during production, use, transportation, storage or disposal.

However, there must be a balance, because one does not want to inhibit economic development by being too focused on security over production. Therefore, decisions should be driven by a calculation of risk. Risk is a function of probability that an incident will occur and the severity of the event. With nuclear incidents, the severity of the event could be quite great, but the likelihood of such an event occurring is low. Whereas with a chemical incident, the likelihood of an event occurring is probably higher and the severity is probably lower. That does not mean that security is not needed. There are a number of different components to a secure chemical system using administrative, operational, engineering, and protective equipment. There are several voluntary codes that include these aspects of chemical control and management. One of the industry codes is the Responsible Care Security Code,[5] which addresses environment, health, safety, and security considerations related to handling of chemicals. Jackson believes that Responsible Care has been so effective and successful in part be-

[3]See BBC News. "Tokyo 1995 Sarin Attack: Aum Shinrikyo Cult Trial Ends." *BBC News Asia*, November 21, 2011. Available at: http://www.bbc.com/news/world-asia-15815056; accessed October 16, 2014.

[4]See Bendavid, N. "International plan calls for removing Syria chemical weapons in months." *Wall Street Journal*, November 15, 2013. Available at: http://online.wsj.com/news/articles/SB10001424052702303559504579200411985935566; accessed September 22, 2014.

[5]American Chemistry Council. Available at http://responsiblecare.americanchemistry.com/Responsible-Care-Program-Elements/Responsible-Care-Security-Code/PDF-Responsible-Care-Security-Code.pdf; accessed September 22, 2014.

cause it combines all of these ingredients. Much of what one can do to make chemical processes safe also makes them secure as well.

In the United States, large companies comply with the Responsible Care Security Code more frequently than do smaller companies. Often a large chemical company will ask another organization to conduct an informal audit to ensure that the company is complying with the code in a kind of "red-teaming" effort. The problem with Responsible Care is that its implementation in particular can be very expensive even though there is a prioritization and assessment of the sites and more security is applied to sites where there are more toxic chemicals or high-pressure situations.

There is another set of codes that has recently been developed for use in smaller chemical and pharmaceutical companies or their contract synthesizers called ChemStewards.[6] These codes also address environment, health, safety, and security. These ChemStewards codes are very helpful for smaller companies.

The U.S. National Association of Chemical Distributors also has a code of management that is very oriented toward making sure that chemicals are distributed in a highly responsible way. Distribution is often where problems of nonstate actors misusing chemicals enter the chemical life cycle. Chemicals are sold to someone thought to be legitimate, but they may not be. Chemicals could then be diverted to make explosives or to make poisons for water or to make drugs, et cetera. In many countries, the distribution system is where the greatest diversion of chemicals occurs. The National Association of Chemical Distributors code states the necessity of always knowing the customer and knowing that the customer is reliable and will take care of the chemicals well. In the United States, some chemical distributors, Sigma Aldrich, for example, have made it a priority to never have the Federal Bureau of Investigation (FBI) find one of their bottles in a methamphetamine laboratory. They are motivated to implement the code thoroughly.

The U.S. government also developed the Chemical Facility Anti-Terrorism Standards (CFATS) in fairly close coordination with the chemical industry. These regulations begin with an assessment of risk on a facility-by-facility basis, determining which chemicals are being used. The Department of Homeland Security (DHS) has identified a number of chemicals that they call "chemicals of concern." If a facility has large quantities of chemicals of concern, then the regulations are to be followed thoroughly. Facilities with fewer chemicals follow the regulations appropriate to their facility. The CFATS are not just for traditional chemical production. Other facilities under CFATS include paint manufacturers and universities. The goal is to not transfer risk to the surrounding community. This is what happened in the West Texas explosion in 2013. When the ammonium nitrate manufacturing facility blew up, a large part of the town was destroyed. In addition, following the explosion, there was some suspicion that there had been attempted

[6]Society of Chemical Manufacturers and Affiliates. "About Chemstewards." Available at: http://www.socma.com/chemstewards/; accessed September 22, 2014.

theft of ammonia, a key ingredient in methamphetamines. If someone were to steal 10 gallons of ammonia, it may not have been noticed at such a large facility. If a person attempting to steal ammonia does not close the valve properly, eventually there will be significant safety problems.

Jackson then discussed vulnerability assessments (VA), which are an aspect of all of the codes she mentioned. The primary goal of a VA is to go through a systematic process to determine vulnerabilities at a particular facility. With this information, facility operators can work to improve security at those points deemed vulnerable to a security breech. A VA does not require sophisticated equipment. She then shared a very typical chemical security risk assessment as an example. First, there is an evaluation of possible threats. Threats may include those who may steal certain chemicals to make illegal drugs or explosives. Second, there is an evaluation of risks posed by those threats. How difficult would it be for that person to break in and either steal chemicals or use them to cause harm at the facility? Third, the risks that were identified must be categorized and adequate responses must be determined. VAs are developed to address security concerns, but the same process can be followed with regard to environmental and safety concerns. To be most effective, VAs need to be conducted in the context of a holistic assessment of the facility. There are several ways this may be done. One may conduct a laptop exercise to determine what might happen if someone broke in. At the other end of the spectrum is performance testing, which involves the facility and the facility security personnel performing their duties in response to mock security threats, which may include force-on-force exercises (with no live fire).

In the United States and in many other parts of the world, there is a considerable effort to make facilities more inherently safe and secure. This is accomplished by substituting more toxic chemicals with less toxic chemicals where possible, developing processes that operate at lower pressures; and minimizing the amount of solvents used, particularly flammable solvents. By using smaller quantities of chemicals and safer chemicals, or by making any necessary highly toxic chemical components on-site to avoid having to transport them, processes and facilities can be more secure. Jackson concluded with an example. Chlorine is a very effective means of purifying water, but it can be, and in fact has been, used as a weapon. Therefore, water purification companies in the United States use peroxide made by using ultraviolet light. Science has helped develop ways to use fewer dangerous chemicals and to keep those we do use them safe and secure.

Current Issues and Possible Solutions to Preventing Accidental or Intentional Chemical Incidents

B. Karthikeyan then provided an overview of the chemical industry in India, followed by an overview of human-caused accidents and incidents, and terrorist acts involving chemicals. The Indian chemical industry is a key part of

economic growth, generating revenue of $108 billion. This figure is expected to reach $224 billion by 2017.[7] To promote development, the Indian government has formed exclusive zones intended only for the chemical industry, where the cluster of chemical industries at the primary plant can supply the downstream units more efficiently.[8] These zones are all located in a central area with developed infrastructure.

Currently in India, there are also about 1,900 Maximum Accident Hazard (MAH) units, many are in the small-scale sector as in any developing nation. Small-scale and medium-scale facilities make up most of the Indian chemical industry. MAH units must follow the Major Accident Hazard Control Rules. Following the accident at Bhopal, a number of changes were made to Indian laws. However, when examining practices on the ground, Karthikeyan sees a gap between laws and implementation. In addition to formal legislation, there are also some voluntary measures taken by the chemical industry itself. The Responsible Care Security Code is now being used in India. Process Safety Management (PSM) still is not mandatory in India, although the government is considering making it mandatory. Many big companies have undertaken Occupational Safety and Health Administration PSM. Concluding the overview, Karthikeyan noted that as the education levels in India increase, media is playing a larger role in raising awareness about the chemical industry because negative perceptions about chemical industries are rampant, just like in any other country.

Karthikeyan then turned to the prevention of accidents. Many of the major accidents that have occurred after Bhopal were caused by human error. The most recent incident, unfortunately, happened just a few months before this workshop in one of the major refineries run by the government of India; 28 people died in the accident. Indian factory rules are from 1947, and while some amendments have been made and some changes are on the way, considerable improvement and modernization of these laws are needed. The end result is that law enforcers do not have proper training on process safety management, which is a critical issue.

Another issue is siting. Chemical industries are given permission to operate in less populated areas, but over time, the population grows to fill in the area surrounding the chemical facilities. When quantitative risk assessments are done, the population is estimated to be a certain size. However, by the time the risk assessment is complete a year later, Karthikeyan said, the population has often dramatically increased, so the whole risk assessment is no longer realistic. There are chemical industries located next to shantytowns, and there are wealthier, well-built houses just next to their compound. What would happen in the event of an accident? From a security point of view, since anyone could rent or

[7]Government of India Planning Commission. "India Chemical Industry: Five Year Plan – 2012-2017." Available at: http://planningcommision.gov.in/aboutus/committee/wrkgrp12/wg_chem0203.pdf; accessed October 16, 2014.

[8]These zones are called Petroleum, Chemicals and Petrochemicals Regions.

build a house very close to the chemical factory, it could be put at considerable risk. Chemical plants are relatively easy targets for terrorists due to the lack of adherence to facility siting rules. Karthikeyan said that this has become such a serious issue now that some privately owned chemical industries are spending their own money on land outside of their boundary walls to create a no-man zone.

Karthikeyan provided the example of the fire in Jaipur at the Indian Oil Corporation's facility.[9] This was a very large oil depot fire. In this incident, the wall of houses were built close to the facility, even though rules mandated that no residences be allowed close to such installations.

A greater focus is placed on occupational health and safety reporting than on process safety, again because small- and medium-scale industries are not required to invest resources in improving process safety. The retirement of employees with years of experience contributes to these challenges. The average age in India is now 27 or 28 years old, which is affecting all industries, especially the chemical industry, because it is considered to be a harsher work environment as compared to the information technology industry or the software industry. This is compounded by a significant knowledge deficit in the chemical industry. The undergraduate curriculum in chemical engineering does not yet address process safety. It is still an elective, not a core subject. Lab-to-plant scale-up is often done without proper study, especially for batch processes; inherent safety is not applied as a means of incident prevention.

Karthikeyan organized his possible solutions into several categories. One is in the area of legislation. In his view, PSM rules need to become mandatory. Then law enforcement must be trained on PSM so that they can enforce the rules. The Chemical Safety Security Rating System also needs to be implemented. This is the new initiative that the government proposed a few months earlier and is in the initial stage of development.

Another solution lies in the area of industry involvement. Currently, there is a lack of sharing of incident databases in India, mainly because industry is worried that if they expose skeletons in their closet they may make themselves more vulnerable. Industry also needs to develop a means of communication with their boards of directors about process risks even if it is difficult. Many times the board does not know what is actually happening at the site, which affects their ability to make decisions. Simulations may be an effective means of conveying the vulnerabilities. This is an area where academia can help, because there are many similar processes. Training simulators are very expensive; therefore a number of chemical industries could jointly fund simulation models required for training. Large- and middle-scale industries should pool their resources, Karthikeyan said. PSM performance ratings should not only be made available to boards of directors, but also to the public.

[9]Oil India Safety Directorate. "M.B. Lall Committee Report, Independent Inquiry Committee Report on Indian Oil Terminal Fire at Jaipur." Available at: http://oisd.gov.in/; accessed October 16, 2014.

Karthikeyan turned to preparation of the next generation of chemical industry employees, saying that undergraduate curricula should require appropriate training. Students and faculty may also provide technical support for small- and medium-scale industries. Karthikeyan observed that throughout India, small- and medium-scale industries do not have resources that academia has for inherent safety and environment safety. There is a need to address the gap in education on all levels that must focus not only on technical ways to improve safety and security at chemical facilities, but also one way to change the mindset of the S&T communities and the general public about the significance of these issues.

Regarding international terrorism, Karthikeyan recounted the incident when a crude oil tank at the Digboi Refinery in northeastern India in 2003 caught fire due to a hand-held missile attack.[10] There are also terrorist threats to the Jamnagar Refinery, which is the largest refinery in India and is located near the border with Pakistan. There have been reports of objects hovering around the refinery. Despite siting rules, terrorists can come quite close to chemical plants. Here there are a variety of vulnerabilities. The first one is the poor quality of roads. India has one of the highest rates of road-related fatalities in the world, approximately 140,000 annually.[11] The government is focusing heavily on road safety, but they have not focused on over-land transport of hazardous materials vulnerable to terrorist attacks. This is one area of deep concern because large quantities of liquefied petroleum gas are transported by oil tankers. These tankers are vulnerable, particularly as they move through heavily populated areas.

Regarding oil and gas pipeline networks, the threats are similar to those in the United States. Pumping stations are in remote locations, and typically there is only one security guard on duty. In addition, the oil and gas pipeline network is expanding. For example, the gas field on the east coast of India will require the construction of gas pipelines leading to southern India.

India has approximately 13 major ports, many of which handle chemicals.[12] Currently, 21 different ministries have some responsibility for these ports.[13] A coordinated approach is needed. Following 9/11, the International Maritime Organization developed a mandatory code called International Ship Port Facility Security (ISPS).[14] All major Indian ports are certified by ISPS. However, there is a safety and security gap. There are a number of fertilizer fac-

[10]Gupta, Barun Das. "Blaze in Digboi Refinery as UFLA Attacks Oil Installation." *The Hindu*, March 9, 2003. Available at: http://www.thehindu.com/thehindu/2003/03/09/stories/2003030905340200.htm; accessed October 17, 2014.

[11]Ministry of Road Transport and Highways, Government of India. "Road Accidents in India 2013, Section I, Accidents on Indian Roads 2013, #2, Recent Trends." Available at: http://data.gov.in/catalo/total-number-persons-killed-road-accidents-india; accessed October 17, 2014.

[12]Das, Pushpita. "Coastal Security – The Indian Experience." Institute for Defence Studies and Analyses. Available at: http://www.idsa.in/system/files/Monograph22.pdf; accessed October 17, 2014.

[13]Ibid.

[14]Ibid.

tories in India, many of which are located on the coasts because some of them import ammonia by ship. Karthikeyan described an example of an ammonia storage tank on the southern coast of India that has a sub-sea pipeline that runs 4.5 kilometers into the sea with a buoy mooring system. Divers pick up the hose, connect it to the ship, and then ammonia is pumped out. This facility is covered under ISPS because it is similar to a port. The storage tank is however exposed to vulnerabilities from the seacoast. This is one area of great concern because there are a number of liquefied natural gas and ammonia tanks located in the coastal areas.

What are the possible solutions? Jackson mentioned security VAs, conducted with common sense and good tools; these should be mandatory in India for chemical security. The existing Manufacture, Storage and Import of Hazard Chemical Rules are mandatory for an established quantity of any of the listed 684 chemicals.[15] Facilities with any of those chemicals could be required to conduct a VA.

Implementation of these laws, regulations, and rules should be enforced, perhaps through surprise drills, security audits, and training. This would require a coordinated approach, which is currently lacking. There are individual steps being made, such as those facilities using the global positioning system to track transport of hazardous chemicals on roads, but currently there is no integrated picture.

Karthikeyan concluded his remarks by recalling the recent attacks on an Algerian facility.[16] One of the lessons learned from the attack was that they had standard operating procedures for terrorist attacks, and they trained on how to respond if there was a terrorist attack. The terrorists hijacked a bus in which employees were coming from their secure residential area, and they attacked and killed a guard. Before the guard died, he activated the terrorist alarm button, and as a result, the plant underwent an emergency shutdown. A major disaster was avoided due to these procedures. These threats cannot be wished away; they are here to stay, and we need to be prepared for them. A great deal of research needs to be conducted because India is a unique mix of cultures and peoples, and there is an equally diverse mix of terrorists around the world.

DISCUSSION

Norman Augustine began the discussion by sharing a hypothetical situation. A company that makes a product wants to produce it safely and securely,

[15]Ministry of Environments and Forests, Government of India. "Manufacture, Storage and Import of Hazardous Chemical Rules, 1989." Available at: http://enfor.nic.in/legis/hsm/hsm2.html; accessed October 17, 2014.

[16]Trindal, Joseph. "Gas Refinery Attack in Algeria: Lessons Learned." Domestic Preparedness Website. Available at http://www.domesticpreparedness.com/Infrastructure/Building_Protection/Gas_Refinery_Attack_in_Algeria%3A_The_Lessons_Learned/; accessed October 17, 2014.

but must make trade-offs in its spending. When trying to explain the trade-offs to the regulator or to the public or to the media, the company wishing not to spend all of its funds on safety and security will be asked: Don't you want to be safe? Don't you want to be secure? This is a difficult position for the person wanting to produce the product to defend. However, security controls can be extreme, and they affect the company's ability to produce the product.

Jackson responded to this scenario by stating that the CFATS have been successful because they were developed with industry as an industry-government partnership. The American Chemistry Council, which is the largest chemical industry association in the United States, worked very closely with DHS to develop those regulations, which made a real difference.

Karthikeyan added that, in India, security for facilities in the public sector is provided by the Central Industrial Security Force (CISF). Regarding private industries, some of them do request the help of CISF, and some of them employ their own private security guards. In trying to address the trade-offs between production and security, cost is important, as is convincing top management that the threat, which they do not see, is important as well. Something that does not happen does not alarm people, and most of the reaction comes after an incident happens. He sometimes refers to this as a risk cataract. The eyes of management may be clouded, and they believe that because nothing has happened, nothing will ever happen. There is tremendous pressure placed on Indian managers, and no doubt on U.S. managers as well, to cut costs. Cutting costs without analyzing its effect on process safety was one of the root causes of the Bhopal disaster.[17] How does one convince management of perhaps the largest challenge after a security VA or a risk assessment of product safety? How does one convince top management that this is necessary? There is still a long way to go.

Another workshop participant asked about how "acceptable risk" is determined. In the case of nuclear plants, there is a tendency to define acceptable risk from a nuclear plant as less than that from a conventional power plant. How does one decide on acceptable levels of risk for chemical plants? Is there a reference point?

Karthikeyan shared his observation that chemical companies focus more on marketing risk and financial risk, and often less on operational risk. All of the large chemical companies have a corporate risk philosophy, but the general tendency is to focus less on process risk. Some large chemical companies in India are developing process risk models based on their overall corporate risk approach, and every company has a different approach.

Michael O'Brien shared his experience that not all VAs are the same. There are some that are more like a checklist with metrics that are often used to determine a particular score, which is either good or not good. In reality, this type of VA does not mean anything when compared with a scenario-based or

[17]Lees, Frank P., ed. *Lees' Loss Prevention in Process Industries.* Volume 3, Appendix 5. Burlington, MA: Elsevier Butterworth-Heinemann, 2005.

performance-based VA. O'Brien asked what type of VA is conducted at chemical facilities in the United States and in India.

Jackson replied that DHS has a vulnerability assessment methodology on their website that must be followed by all Tier-1 through Tier-4 facilities in the United States. This produces some consistency in assessments, which are both scenario based and performance based. She was uncertain as to whether or not insider threat analysis is included in the DHS VAs. Some of these simulation exercises would be appropriate for cooperation between Indian and U.S. experts.

Karthikeyan continued that India is still at the very initial stages of developing VAs. Basic checklists are being completed by typical security agencies looking at intrusion prevention. India still has a lot to learn from American experience and the CFATS Tier-1, Tier-2, and Tier-3 facilities. In India, improving process safety is the primary focus and security is slowly being addressed. He also agreed that the issue of insider threat analysis is important to address with regard to VAs in India because the country will face a shortage of 14,000 chemical engineers over the next 5 years. Approximately seven to eight million skilled people will be needed in the industry.[18] The practice of performing background checks on those who enter this workforce has not yet started in India to Karthikeyan's knowledge.

In reference to management cutting costs, a participant stated that the government of India and the state governments have an overall responsibility for the welfare and safety of its citizens. Particularly after the disaster at Bhopal, there should be rules and regulations in place that require a company to conduct risk assessments approved by the government. Assessments should address two aspects of risk: the risk to the public and to the people living nearby, and the risk to the facility employees. It is surprising that so many years after Bhopal, the government would not have developed regulations and would give this discretion to companies. The other problem is that cost cutting occurs at the unit level. For example, in the BP Texas City Refinery disaster, the BP board in London passed a directive to cut 25 percent of fixed costs in all of their refineries, so units started cutting costs. It is the responsibility of the unit to explain the risk involved in cutting those costs to boards of directors.[19] This communication is currently inadequate.

Karthikeyan replied that after the Bhopal disaster, one of the regulations that was changed pertained to publicly held companies. Under this regulation, someone on the board of directors is classified as an "occupier." The occupier can be criminally prosecuted for any accident that happens in any facility owned

[18]National Skill Development Corporation. *Human Resource and Skill Requirement for the Chemical and Pharmaceuticals Sector (2022). A Report*. Available at: http://www.nsdcindia.org/pdf/chemical-pharma.pdf; accessed on October 24, 2014.

[19]U.S. Chemical Safety and Hazard Investigation Board. "Investigation Report: Refinery Explosion and Fire (15 Killed, 180 Injured), BP, Texas City, Texas, March 23, 2005." Available at: http://www.csb.gov/assets/1/19/CBSFinalReportBP.pdf; accessed October 17, 2014.

by that company.[20] The positive aspect he has seen over the last 5 years is the number of criminal prosecutions of 'occupiers' who are primarily board directors of companies is increasing. This is a visible sign that enforcement is occurring.

An additional challenge is in enforcement of existing regulations. Karthikeyan stated that safety inspections do take place; however, one of the largest issues the enforcing authorities face is the lack of an adequate number of people who can serve as inspectors. Corruption is also a significant issue. On the other hand, there are people who genuinely do their job, but they are stretched to the limit. They cannot cover all of the industries. It is a very fluid situation where nothing is entirely known. Although India has a large workforce, there needs to be a clear intention on the part of the government to implement these regulations and to hire and train adequate professionals to ensure this implementation.

Rita Guenther asked a question regarding whether or not there are threshold limits placed on the quantities of chemicals allowed for sale to a particular type of customer. For example, if one were to accumulate a large amount of chemicals in smaller batches, would anyone detect that? How are Internet sales tracked if there are thresholds? Her second question pertained to priority areas for scientific cooperation between India and American experts to address the gaps that need to be addressed.

Jackson replied to the question regarding threshold limits on sales and purchases of chemicals. In any chemical regulation, whether it is the United Nations Chemical Weapons Convention or the U.S. Anti-Chemical Facility Anti-Terrorism Standards Authorization and Accountability Act, there is always a threshold regarding sales of chemicals. However, there are also other various thresholds, including for storage, use, purchase and transportation, and these become extraordinarily complicated. Regarding cooperation, a critical area is that of teaching a culture of safety and security. U.S. universities have not been very good at developing even a culture of safety within chemistry departments until very recently, after there were several deaths due to very bad accidents.

With regard to scientific cooperation in this area, Karthikeyan offered three prioritized areas related to terrorism. One would be sharing experiences about security and VAs, especially how they have been conducted and what has been learned through the process of having conducted these analyses. A second priority area for cooperation is road transport. How can experts prepare for responses to terrorist attacks on hazardous materials? This is an area in which Indian experts can learn from American colleagues, particularly those who have been involved in the establishment and development of DHS. The third priority area for cooperation involves the best ways to manage a myriad of law enforcement agencies.

[20]The Factories Act, 1948 (Act No. 63 of 1948), as amended by the Factories (Amendment) Act, 1987 (Act 20 of 1987). International Labour Organization. Available at: http://www.ilo.org/dyn/natlex/docs/WEBTEXT/32063/64873/E87IND01.htm#a085; accessed October 17, 2014.

AGRICULTURAL AND FOOD SECURITY

Recent Indian and American Experiences in Cooperating on Food Security

Vedpal Yadav presented approaches of the U.S. Food and Drug Administration (FDA), based on his close collaboration with FDA, in his experience with food security in India. Yadav dedicated his talk to the more than 20 children who died from contaminated food in an incident in Chapra, Bihar, in 2013. He began by making distinctions among food safety, food defense, and food security. Food safety encompasses the efforts to prevent accidental (unintentional) contamination of food products (see Figure 3-1). Food defense encompasses the efforts to prevent intentional contamination of food products (i.e., human intervention as the source of contamination). Food security is a term that is now used more broadly to include both physical and economic access to food that meets people's dietary needs. The World Health Organization defines food security as being achieved when all people at all times have access to sufficient, safe, nutritious food to maintain a healthy and active life.[21]

FIGURE 3-1 Food safety includes efforts to prevent accidental (unintentional) contamination of food products. A contaminated mid-day school meal was the result of a food safety accident and killed more than 20 children in Chapra, Bihar, India, on Tuesday, July 17, 2013. SOURCE: Yadav, 2014.

[21]World Health Organization. "Rome Declaration on World Food Security and World Food Summit Plan of Action." World Food Summit, November 13-17, 1996. Available at: http://www.fao.org/wfs/index_en.htm; accessed September 18, 2014.

Yadav said that there is a spectrum of motives for intentional food contamination, from extremist groups to economically motivated adulteration (the melamine in Chinese milk is an example). He pointed out that the food supply is a soft target for terrorists because contamination of the food supply has the potential to cause significant health consequences, to cause widespread public fear, and to adversely affect the economy, leading to food insecurity. The complex nature of the food supply, with many inputs and outputs, makes it particularly vulnerable to intentionally introduced contaminants. Furthermore, such incidents of contamination may easily spread across international boundaries because in the 21st century, the food supply chain is truly global. The United States Department of Agriculture (USDA) has conducted vulnerability assessments that demonstrate that a deliberate contamination of the food supply has the potential to cause mortality rates from 1,000 to up to 300,000 deaths depending on the commodity, the agent used, and where in the supply chain the contaminant was added. Beyond the immediate health effects, such incidents could have a devastating effect on the economy, into the billions of dollars,[22] and cause widespread fear.

Yadav stated that the problem is particularly complex in the United States, where approximately 75 to 80 percent of seafood is imported, 50 percent of fresh fruits are imported, and agricultural imports are close to $80 billion annually. Further, in the United States, agriculture accounts for about $1.24 trillion of the gross domestic product, and about 2 percent of all U.S. jobs (held by 24 million Americans) are directly employed in the agricultural sector, and one in six U.S. jobs are related to agriculture.

Contamination can occur at any point in the food chain: in the crop-growing stage or as a result of contaminated livestock, and the food-processing distribution, storage and transportation phases are also at risk of intentionally or unintentionally introduced contamination. There is a wide variety of intentional and unintentional contaminants about which experts worry. Unintentional contaminants include *Escherichia coli, Salmonella, Listeria monocytogenes,* pesticide residues, polychlorinated biphenyls, and furans; intentional contaminants include *Bacillus anthracis* (anthrax), *Clostridium botulinum* toxin*, Yersina pestis* (plague), arsenic, cyanide, ricin, plutonium-238, and cesium-137.

Yadav emphasized that there is a great deal that can be learned from food safety related to outbreaks, and these lessons can be applied to food defense scenarios. An unintentional incident, for example, can tell us what impact an intentional contamination incident may have on the food supply, on public health, and on public reaction. He provided the example of an unintentional incident that occurred in the United States in September 1994, when an estimated

[22]Based on USDA estimations on the economic value of food-related industries. See, for example, USDA, Economic Research Service. "Ag and Food Statistics: charting the Essentials." Available at: http://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-essentials/ag-and-food-sectors-and-the-economy.aspx#.VBtkiGMcXYA; accessed September 18, 2014.

224,000 people became ill when ice cream was contaminated with *Salmonella* serotype Enteritidis.[23] Hospitalization was required for 30 of 112 patients.[24] The ice cream was produced at a single facility, and was most likely contaminated in transit when the pasteurized ice cream mix was transported in a truck that had previously carried raw liquid eggs. Further, on July 27, 2013, an unintentional incident occurred in Chapra, Bihar, India, when a contaminated midday school meal killed more than 20 children. The cause of the incident was determined to be organophosphorous pesticide mixed in cooking oil.[25]

The United States also experienced an intentional incident in 1984, when a cult member introduced *Salmonella* bacteria into restaurant salad bars. The intent of the perpetrators was to affect the outcome of a local election and resulted in 751 reported illnesses, and the hospitalization of 45 people (see Figure 3-2).[26]

FIGURE 3-2 Food defense encompasses efforts to prevent intentional contamination of food products. In 1984, cult members in the U.S. state of Oregon added *Salmonella* bacteria to restaurant salad bars. SOURCE: Yadav, 2014.

[23]Hennessey, T.W., et al. "A National Outbreak of Salmonella enteritidis Infections from Ice Cream." *New England Journal of Medicine*, vol. 334, no. 20, May 16, 1996. Available at: http://www.nejm.org/toc/nejm/334/20; accessed September 18, 2014.

[24]Ibid.

[25]BBC News India. "School Meal Kills 22 in India's Bihar State." *BBC News India*, July 17, 2013. Available at: http://www.bbc.com/news/world-asia-india-23337445; accessed October 17, 2014.

[26]Torok, Thomas, et al. *A Large Community Outbreak of Salmonellosis Caused by Intentional Contaimination of Restaurant Salad Bars*. Centers for Disease Control and Prevention. Available at: http://www.cdc.gov/phlp/docs/forensic_epidemiology/Additional%20Materials/Articles/Torok%20et%20al.pdf; accessed October 17, 2014.

Fortunately there were no fatalities linked to this incident. Although the outbreak was detected by local public health officials, it took the FBI about 1 year to link the outbreak to the cult headed by Bhagwan Shree Rajneesh. The investigation was complicated by the fact that it was difficult to actually determine whether the contamination was intentionally introduced, because the same microbe causes many unintentional contaminations.

While the Oregon incident is the only confirmed case of intentionally introduced contamination in the United States, the threat remains real, as indicated by the 1989 threat of contaminated grapes entering the United States from Chile.[27] A terrorist group phoned the U.S. Embassy in Santiago, Chile, claiming to have contaminated Chilean grapes with cyanide. Supermarkets pulled Chilean fruit off the shelves throughout the United States, and consumers received a warning not to eat any fruit imported from Chile. Most of the peaches, blueberries, blackberries, melons, green apples, pears, and plums on the U.S. market at the time were imported from Chile. The incident devastated an entire season of fruit sales from Chile at a cost of $200 million in lost revenue.

This case demonstrates the threat from economically motivated adulteration (EMA). EMA is defined as fraudulent, intentional substitution in or addition of a substance to a product for the purpose of increasing the apparent value of the product or reducing the cost of its production for economic gain. There are several factors that contribute to EMA, including the following:

1. In an expanding global marketplace, more food is moving across international borders than ever before.
2. Companies may have less control over processes due to the global supply chain.
3. Each year of the past 7 years, food imports have grown by an average of 10 percent.
4. Tighter economic conditions lead to price increases that in turn drive fraudulent activity.
5. Global food shortages create rising demand for food creating imbalances in the marketplace.

Yadav then provided specific examples of EMA events. In 1995, unapproved pesticides were used that entered the food supply via cereal, causing $140 million in loss of sales.[28] In 2004, there was an incident in which unapproved dyes were used in Indian spices, which resulted in a recall and the loss of

[27]Shenon, P. "Chilean Fruit Pulled from Shelves as U.S. Widens Inquiry on Poison." *New York Times*. March 15, 1989. Available at: http://www.nytimes.com/1989/03/15/us/chilean-fruit-pulled-from-shelves-as-us-widens-inquiry-on-poison.html; accessed September 21, 2014.

[28]Villani, Joe. "Pesticide Testing: What's the Best Way?" *Food Product Design*. February 1, 1995. Available at: http://www.foodproductdesign.com/articles/1995/02/pesticide-testing--whats-the-best-way.aspx; accessed September 20, 2014.

$300 to $500 million in sales.[29] In 2008, a Chinese milk producer, Sanlu, sold milk contaminated with melamine, affecting 290,000 people and killing 6 people (mostly children).[30] Due to its high nitrogen content, milk producers added melamine to powered infant formula in order to falsely increase the protein content of the food. The Sanlu plant consequently went bankrupt and the milk industry lost $5 billion in sales.[31] A similar incident occurred in 2009 with peanuts sold by the Peanut Corporation of America. In that case, a *Salmonella* contamination was intentionally concealed by management and the market for the affected product dropped by 25 percent, resulting in a $1 billion impact.[32] In 2012, fraudsters purchased bottles for a premium line of ketchup, and filled them with basic, cheaper ketchup.[33] Without adequate food safety measures, the bottles fermented and exploded. The operation was then abandoned and neighboring companies reported foul smells and vermin in the area.

Yadav noted that the food supply is vulnerable to cyberattacks as well. Some food companies rely on computer systems to control food manufacturing processes. Given the heightening focus on cybersecurity, all sectors should be adequately protected. Companies in the food chain are vulnerable, and Symantec, a cybersecurity company, estimates that more than 80 percent of small businesses do not have a formal cybersecurity plan, and a typical cyberattack on a small business could cost $200,000, subsequently threatening the solvency of the company.[34] To address these cyber-threats, companies should use password-protected facility computers, install firewalls on computer networks and use up-to-date computer virus protections and detection systems, train personnel with access to critical cyber assets to recognize and report indicators of insider

[29]See, for example, Ehling, S. "Consumer Product Fraud: Deterrence and Detection." Presented at the Ozark Food Processors Association Annual Convention, April 6, 2011. Available at: http://ofpa.uark.edu/pdf_files/2011%20talks/Ehling%20Product%20Fraud.pdf, p. 6; accessed September 26, 2014.

[30]Yardley, Jim. "Chinese Baby Formula Scandal Widens as 2nd Death is Announced." *New York Times*, September 15, 2008. Availability at: http://www.nytimes.com/2008/09/16/world/asia/16milk.html?_r=0; accessed October 20, 2014.

[31]Grocery Manufacturers Association and A. T. Kearney. *Consumer Product Fraud: Deterrence and Detection*, 2010, p. 6. Available at: http://www.gmaonline.org/downloads/research-and-reports/consumerproductfraud.pdf; accessed September 26, 2014.

[32]Tavernise, Sabrina. "Charges Filed in Peanut Salmonella Case." *New York Times*, February 21, 2013. Available at: http://www.nytimes.com/2013/02/22/business/us-charges-former-owner-and-employees-in-peanut-salmonella-case.html?adxnnl=1&adxnnlx=1413813790-kAVmhbQe821N3N+ptvx12Q; accessed October 20, 2014.

[33]Tepper. R. "Counterfeit Heinz Ketchup Operation Discovered in New Jersey." *Huffington Post*, October 18, 2012. Available at: http://www.huffingtonpost.com/2012/10/18/counterfeit-heinz-ketchup_n_1981324.html; accessed September 22, 2014.

[34]Brooks, C. "Small Businesses Don't Take Cybersecurity Seriously." *Business News Daily*, October 26, 2011. Available at: http://www.businessnewsdaily.com/1603-cybersecurity-small-business.html; accessed September 22, 2014.

threats, limit physical access to computer systems to authorized personnel, and have policies and procedures for handling an insider threat incident.

To combat these threats to the food supply, the United States uses a comprehensive strategy to address various aspects of food defense. These strategies are codified in laws and directives, and contain the following elements:

1. Outreach: The approach to outreach and training for industry and consumers is to provide information and tools to assist them in addressing food defense. This includes guidance materials on food defense plans and exercise kits. Training is also provided for agency employees, relevant partner agency personnel, and foreign counterparts.
2. Vulnerability Assessments: VAs are performed for various commodity systems, which help identify products of higher concern, points in the process that are more vulnerable to intentional contamination, likely agents that could be used, mitigation strategies for government and industry, research needs, and a means of better allocating limited human and financial resources.
3. Mitigation Strategies: The FDA works closely with the food industry, partner agencies, and foreign counterparts on developing and implementing mitigation strategies.
4. Surveillance Activities: Surveillance activities are performed in various ways, such as by sampling some food products for certain threat agents, consumer reporting systems, and suspicious activity reporting.
5. Research: Research is conducted on food defense needs, such as developing detection methods and survivability studies of threat agents in food processing.
6. Food Defense Exercises: Food defense exercises are performed to test response plans and include industry and government stakeholders. These exercises contribute to the development of guidelines for industry on food disposal and facility decontamination. It is important to understand that food may be considered hazardous waste depending on the contaminant, and therefore special disposal methods may be necessary. Typical sanitation cleansers may not be sufficient to ensure that the facility is free of residue before resuming food production.
7. Media Involvement: Good relationships with the media are critical to ensure informed reporting that can aid quick recovery from an incident. It is important to understand that heightened interest by the public and media requires special consideration when developing risk communication messages.

In conclusion, Yadav summarized his remarks by stating that there is a broad spectrum of nontraditional threats to the food supply chain, and it is possible to cause significant public health and economic impact from intentional contamination. Therefore, experts must focus on the entire food supply chain, "farm to fork." To do so effectively requires the development of a comprehen-

sive strategy and collaboration with all stakeholders. The food supply is global, and experts must work together to reduce and minimize the risk and impact of an incident of intentional contamination.

Securing Plants, Animals, and Crops in India

Abraham Verghese specifically addressed the threat to agricultural crops from invasive species entering India mostly in an unplanned manner. Compared with other threats, the perceived threat from invasive species is low, and methods of preventing the arrival of these species are weak. However, once an invasive species is identified, India's capacity to address the invasion is good.

Verghese then described several threats that Indian agriculture faces due to invasive species. The first was the western flower thrips (*Frankliniella occidentalis* [Pergande]). This insect is native to North America and punctures the leaves, flowers, or stems with its mouth and sucks the sap of the plants. The *Phenacoccus manihoti*, a bug that affects Africa and Thailand, caused crop losses of up to 82 percent in the 1980s and in 2008.[35] The *Brontispa* beetle can potentially enter India from all sides and affect coconut trees by damaging their crowns and eventually killing the entire tree. In 2006 and 2007, the beetle caused considerable damage in Myanmar.[36]

The *Ophelimus maskelli* (bug) is threatening to become an invasive species from Europe, and the *Aleurodicus dugesii* (giant whitefly) is a potential invasive threat to India from Mexico.[37] The glassy-winged sharpshooter leafhopper (*Homalodisca vitripennis*) is native to the south eastern United States and is a vector for bacterium (*Xylella fastidiosa*), which causes devastating plant diseases, such as Pierce's disease and scorches.[38] The Mediterranean fruit fly (*Ceratitis capitata*) can be found in most tropical and subtropical areas of the world and is the world's most destructive pest. Unlike most fruit flies, it can tolerate cooler climates and live on a wide range of host plants, such as apricots, nectarines, peaches, mandarins, and to a lesser extent apples and pears. Wheat stem rust (Ug99 race) is a continuing problem in India, and globally 80 percent

[35]Lyons, Elizabeth E. and Scott E. Miller. "Invasive Species Eastern Africa: Proceedings of a Workshop held at ICIPE, July 5-6, 1999." African Insect Science for Food and Health (ICIPE) Science Press. Available at: https://www.cbd.int/doc/meetings/cop/cop-05-inf-33-en-pdf; accessed October 20, 2014.

[36]Invasive Species Compendium. "Datasheet: Brontispa Longissima." Available at: http://www.cabi.org/isc/datasheet/10059; accessed October 20, 2014.

[37]Drake, James A., ed. "Handbook of Alien Species in Europe, Invading Nature – Springer Series in Invasion Ecology." Vol. 3, 2009. Available at: http://www.springer.com/life+sciences/ecology/book/978-1-4020-8279-5; accessed on October 20, 2014.

[38]Mizell, Russell F., et al. "Xylella Fastidiosa Diseases and Their Leafhopper Vector." University of Florida. Available at: http://edis.ifas.ufl.edu/pdffiles/IN/IN17400.pdf; accessed October 20, 2014.

of wheat varieties are susceptible.[39] Based on prevailing winds and areas of wheat production, the most likely route for the continuing advance of wheat rust is via the Arabian Peninsula.

Verghese provided examples of how other plants and insects have been introduced as a means of countering invasive species. The water fern (*Salvinia molesta*) is a native of south eastern Brazil, and to counter this species, *Cyrtobagous salviniae* was introduced from Australia in 1982; large-scale mechanical removal of the fern was avoided, and the waterways were restored for transport and irrigation.[40] The water hyacinth, *Eichhornia crassipes*, is also a native of Brazil and was introduced as an ornamental plant in the Calcutta botanical gardens in 1895.[41] In 1982 and 1983, *Neochetina bruchi*, *N. eichhornia*, and *Orthogalumna terebrantis* were introduced from Argentina.[42] Similarly, *Alternaria* was found to be particularly effective in combination with arthropods to combat weevils and mites, which are well established in India and which spread rapidly.[43]

Verghese said that 40 percent of insect invasions occur in the country through plant materials, 25 percent are from timber imports and 35 percent are accidental.[44] Many of the ports of entry into India are porous with respect to plant products. These species could come across the border or be brought via seafaring trade, causing significant impact to agriculture and biodiversity, food supplies, commerce, and the economy.

Verghese closed by noting existing initiatives developed to address the global problem of invasive species, and steps that India plans to take to limit the

---

[39]Consultative Group on International Agricultural Research. "Virulent a New Strains of Ug99 Stem Rust, A Deadly Wheat Pathogen." May 28, 2010. *ScienceDaily*. Available at: http://www.sciencedaily.com/releases/2010/05/100526134146.htm; accessed on October 20, 2014.

[40]Wittenberg, Rudiger and Matthew J.W. Cook, eds. "Invasive Alien Species: A Toolkit of Best Prevention and Management Practices." Invasive Species Specialist Group Website. Available at: http://www.issg.org/pdf/publications/GISP/Guidelines_Toolkits_BestPractice/Wittenberg&Cock_2001_EN.pdf; accessed October 20, 2014.

[41]Hastings, R.B. "The Relationships Between the Indian Botanic Garden, Howrah and the Royal Botanic Gardens, Kew in Economic Botany." Royal Botanic Gardens Website. Available at: http://www.kew.org/collections/ecbot/pages/wp-content/media/papers/hastings1986howrah.pdf; accessed October 20, 2014.

[42]Jimenez, Maricela Martinez. "Progress on Water Hyacinth (*Eichornia crassipies*) Management." Available at: http://www.fao.org/docrep/006/y5031e/y5031e0c.htm; accessed October 20, 2014.

[43]Walia, Suresh and G.S. Dhaliwal. "Essential Oils as Green Pesticides: Potential and Constraints." *Biopesticides International*. 4(1): 63-64. (2008). Available at: http://www.sierranaturalscience.com/THYME_CLOVEOIL.pdf; accessed October 20, 2014.

[44]Sallam, Mohammad N. "Insect Damage: Damage on Post-Harvest." Food and Agriculture Organization of the United Nations. Available at: http://www.fao.org/fileadmin/user_upload/inpho/docs/Post_Harvest_Compendium_-_Pests-Insects.pdf; accessed October 20, 2014.

damage caused by invasive species.[45] The Rio Convention on Biological Diversity of 1992 was an effort to raise awareness of the real threat posed by these species and to call for greater action to limit their transfer. The United Nations and other international organizations also formed the Global Invasive Species Program to answer this call with a series of programs designed to deal with particular sorts of introduced species. The International Union for Conservation of Nature (IUCN) has identified the problem of alien invasive species as one of its major global initiatives and recently finalized the IUCN Guidelines for the Prevention of Biodiversity Loss Caused by Alien Invasive Species.[46] India plans to tackle the domestic problem of invasive species by developing a process of strict quarantines like those in the United States and Australia. Given its importance, they plan to raise the level of awareness about invasive species among the general public.

DISCUSSION

The discussion began with a question about what happens to species that are intentionally introduced into India to try to counter invasive species. Verghese replied that these species remain in the ecosystem; therefore, it is important to be careful about what is introduced, where, and why. The goal is to identify a species that only targets the intended species and does not adversely affect any of the other native species.

Raymond Jeanloz asked a question in this session that applies to all sessions. When is the situation good enough? In other words, at what point does one decide that additional investments in security are not worth the additional marginal benefits? There must be some analysis in the food industry of the point at which companies will not spend more money on making the food supply safer. From a technical point of view, it is important to ask the question about what is good enough. How should we assess the tradeoffs in terms of how good the security and safety have to be for us to agree that it is good enough? Yadav replied that in the food supply in the United States, all industries are governed by a regulatory body that enforces regulation and the expected outcomes of the food industry. Compliance with these regulations is easy for large, multinational corporations, but it is difficult for small companies, such as those in India because the necessary equipment is expensive. Therefore, he noted that the guiding principle is a common-sense approach.

Verghese added that tradeoffs exist unwittingly because at the points of entry into India, greater attention is paid to the import of non-biological products

[45]Botanic Gardens Conservation International. "Agenda 21: Programme of Action for Sustainable Development Volume 3, Number 2." June, 1999. Available at: http://www.bgci.org/worldwide/article/0011/; accessed October 20, 2014.

[46]McNeely, Jeffrey A., et al. "Global Strategies on Invasive Alien Species." U.S. Fish and Wildlife Service. Available at: http://www.fws.gov/invasives/volunteerstrainingmodule/pdf/bigpicture/globalstrategy.pdf; accessed October 20, 2014.

such as gold and silver, and to electronic goods than to foods and plants. India is trying to create a better balance so that financial investments in security will be better focused on potential threats. It is important to develop more economic analysis to guide decisions about investments in security. Jeanloz added that at this point, profit has greater weight than security considerations, although there are cultural issues as well. For example, what would India be like without coconuts? Therefore, he wanted to start the discussion about the potential qualitative consequences of terrorism in addition to financial consequences. Verghese agreed with Jeanloz's point because, as he recounted, when the invasive species affected the coconuts, the local government was toppled. Yadav also noted that the tradeoff is similar to that made regarding insurance: "How much insurance is sufficient?" Investment in food defense is like an investment in insurance. Another workshop participant noted that this discussion is an important outcome of the workshop.

A workshop participant asked how one would determine whether an incident was caused intentionally or unintentionally. Yadav replied that the answer to this question deals with the distinctions between food safety and food defense. There are only two factors that differentiate these issues. The first is whether or not the contaminant is naturally occurring in the food supply, such as *Salmonella*. If it is, this is considered food safety. Food defense deals with intentionally introduced substances that are not part of the food supply chain, such as anthrax. The participant followed up with a question as to whether or not there were examples of an intentional outbreak caused by a naturally occurring substance. Yadav noted that in 1984, a cult in the United States introduced *Salmonella* into salad bars and during the investigation, the chain of custody was traced to determine how the *Salmonella* was introduced.

Augustine raised the issue of insider threats. The food defense plan showed by Yadav did not specifically site the insider as a potential threat. He asked what is being done today to address the insider threat. Yadav replied that this was discussed during his training in the United States, and he learned that employees in food industries undergo background checks. In the food defense plan, there are mechanisms for supervisors and managers to report employees who may exhibit unusual behavior, if there is such an employee, he or she will remain under surveillance until there is a change in behavior or in the situation.

David Franz asked how good the United States is at tracking food back through the food supply chain and how important this ability is for food safety and food defense. Yadav answered that most U.S. industries are regulated by USDA, and they are about 90 to 95 percent compliant. These industries also have surveillance systems to determine what happened in the event of an incident, but it is not foolproof. Franz followed up by asking if there is one comprehensive database with all food items available in U.S. supermarkets. For example, if a customer buys a tomato from China, can he or she go back to find the place of origin of the tomato? Yadav replied that the chain of custody is maintained at every point on the supply chain, but it is not easy to trace. Verghese added that there are national standards established by each country that regulate

international imports and exports of food stuffs and whether or not the imports and exports comply with the regulations.

Van Romero noted that public perceptions are also important. The government can say whatever it wants, but if a consumer does not want to buy something, he or she will not. This was true after the Fukushima nuclear disaster, for example. Some people in the United States would not believe that the food was safe, even though many tests had determined it to be radiation free. Yadav agreed that countries need to explore their trade offs in regard to investment in public outreach.

Guenther asked about the distinction between intentionally introduced and unintentionally introduced contaminations of elements common into the food chain. A terrorist may intentionally introduce a naturally occurring contaminant into the food supply chain to avoid detection or suspicion. Likewise, terrorists may not always be looking for maximum casualties. The whole point may be to keep people sick for a long time, meaning that an intentionally introduced contaminant that is part of the normal food chain may go undetected for a long time.

Yadav replied that if regularly occurring contaminates are introduced into the food chain at a high level, they will not go undetected. The first point of detection would be at the processing stage, because industry regularly checks for contaminants that are normally part of the food chain. In the case of salad bars, analyses of pathogens that are part of the food chain are taken regularly. However, as with anything else, there are outliers, and these incidents should be detected at public health institutions and an investigation would be launched. These incident reports would signal that something is amiss. Unfortunately, unless someone reports something to hospitals, these incidents could go undetected.

Finally, Guenther asked how Indian experts identify invasive species. Verghese noted, as an example, that the beetle populations in the northeast of India are monitored due to the border with Myanmar, where the beetles are rampant. They have developed a system whereby there is a central agricultural university in the region with affiliates down to the local level. Local communities are shown how to identify the beetles and why they are important to locate, and people then look out for them, and if there is any suspicion of an increase in the number of beetles, people are to alert the network and a response team is sent. They are considering introducing training to children, because this has been successful in Australia, where almost all school children know about invasive species; starting awareness with children is effective because young people like to catch bugs and are curious about the natural world.

PROTECTING CRITICAL INFRASTRUCTURE

Enhancing the Security of India's Critical Infrastructure: Aviation Security

B. K. Maurya began his presentation by noting that since 9/11 and the December 1999 Kandahar hijacking incident, aviation security has undergone a radical shift in India. Aviation is a global industry, and as aviation security con-

cerns have grown globally, mutual cooperation has grown among countries. India has enacted stringent measures to ensure that international regulations are followed with respect to cargo and passenger security. At the same time, air travel has increased dramatically in India to previously unimagined levels: nearly 160 million passengers flew through Indian airports in 2012. To enhance professionalism in security operations in India's civil aviation sector, 51 airports in the country have been placed under the Central Industrial Security Force (CISF).

Security, Maurya noted, always comes with trade-offs among cost, privacy, and facilitation (ease of passage). Due to the increasing costs of aviation fuel, the profit margin on commercial flights is low, Maurya said, and this creates pressures on the costs of security, as they compete against profits. To detect and identify threats, baggage and passengers are screened, which takes time. Expectations vs. realities must be balanced with respect to risk.

The main threat focus in the aviation sector is on improvised explosive devices (IEDs) and prohibited items (weapons and hazards), but given the complexity of the aviation enterprise, cybersecurity, insider threats, vehicle bombs, and other threats also demand attention. Innovative technology may help address the challenges faced in air security. Maurya highlighted technologies currently used in aviation security in India, including surveillance equipment, perimeter security equipment, biometric access systems, X-ray screening systems for cargo, explosive trace-detector systems for explosives in cargo and baggage, and canine explosive-detecting teams. Security managers are considering ideas such as blast-resistant cargo containers (or wrapping cargo containers in bomb blankets), more formal Perimeter Intrusion Detection and Assessment System systems, more sophisticated x-ray scanners, such as computed tomography scanners, neutron-based screening technology, detectors for liquid explosives, and IED disruptors.

Maurya affirmed that India also takes the human side of aviation security, and particularly insider threats, very seriously, and said several steps have been taken to address this potential problem.

Recent Experience with Averted Power Failure in Silicon Valley

Michael O'Brien began by noting that, historically, critical energy infrastructure in the United States has operated in a low-threat environment. However, the perception of the threat environment has changed as cyberattacks have steadily increased in recent years, and two incidents in 2013, one in the state of California and one in the state of Arkansas, demonstrated how significant damage could result from orchestrated physical attacks. As a result, DHS, the Department of Energy, and the FBI are working closely with U.S. industry to communicate current threats and discuss enhanced protection measures to mitigate attacks from a higher threat.

Protecting energy supplies worldwide is extremely important. U.S. reliance on electricity is pervasive; very few activities and operations work without

electrical power. The threat to critical infrastructure is a global problem, and lessons learned through critical infrastructure protection work can be applied globally.

On April 16, 2013, a group sabotaged an electrical transmission facility in California's Silicon Valley. The attackers caused significant damage (estimated at $20 million), but a blackout was averted. Four months later, in three sabotage attacks, power lines and power poles were cut down and a control center was burned in Arkansas.

O'Brien stated that although technology solutions are important to protect critical infrastructure, they are not the only answer. Sometimes the solution is better on-site situational awareness (more guards or monitors) and better coordination between guards and local law enforcement authorities. Wherever technology is used, it has to be selected and integrated with the facility and the organization using the technology, and it has to be maintained. Classifying threats as low, medium, and high, he said that the costs to protect against threats will increase exponentially as they move from low to high. Critical infrastructure generally has industrial-level security, which is inadequate against a higher threat.

O'Brien's group at Lawrence Livermore National Laboratory conducts vulnerability assessments and helps to develop security plans for key facilities. He and his colleagues evaluated the 2013 attacks and made recommendations. His group also advocates a systematic approach to both evaluate security at the facility and to develop a graded protection strategy made up of layers of security measures.

O'Brien said that the first step is to define the design-basis threat and to develop a list of adversary characteristics. A clear understanding of current threats and the mitigation of risks in a critical industrial environment is essential. Next, his team characterizes the facility and identifies targets. Based on these definitions and characterizations, they develop attack scenarios and validate them to ensure that the scenarios represent the key security needs. O'Brien and his colleagues then identify measures to mitigate the vulnerabilities and then validate those measures, modeling attacks with the mitigation measures in place. Finally, they analyze the costs and benefits of the measures to support decisions about whether to deploy the mitigation measures.

At any facility, one also needs to have an effective insider protection program to promote security culture. Identification of critical facilities and understanding cascading effects of attacks, he said, are key to defining consequences, as is deployment of protection strategies that integrate human and technology elements to mitigate risk.

A Practical Approach to Infrastructure Protection: Lessons from the Field

John Holmes provided a practical, experience-based approach to infrastructure protection; in essence, he distilled lessons learned from several years as

director of operations and security at the Port of Los Angeles, where approximately $200 million have been spent on security upgrades since 2001. The combined Los Angeles-Long Beach Port Complex is the world's fifth largest port, with 25,000 employees who handle 43 percent of U.S. container imports using the port's ships, channels, waterways, bridges, roads, rail facilities, power stations, and other facilities. Major ports are not only critical infrastructure themselves, they are cities with critical infrastructure of their own.

Holmes said that development and implementation of security systems for critical infrastructure is sometimes described in four steps: define the requirements, design the protection system, evaluate the system once installed, and repeat as needed. But it is never that simple for complex facilities. Security is a system of systems in which all the pieces must fit together to be effective, but business operational processes conspire to thwart system development. Vulnerabilities are created when some of the pieces do not fit together or into the larger system. Regardless of the technical aspects of security, the implementation, integration, maintenance, and management of systems present the largest challenges.

Holmes noted that an important feature of an effective security organization is the ability to learn from mistakes, adapt, and improve. He listed 10 lessons he learned while securing the Port of Los Angeles, saying that he hoped no one would have to repeat the mistakes that taught him these important lessons. The 10 lessons are:

1. *Identify your problems*. Conducting a security assessment enables the security manager to focus on the most important problems and to justify use of funds to address those problems. Assessment is not a one-time event; it should be conducted continuously to ensure that it is current and that it responds to changes in the global and local threat and physical environment. Cybersecurity was not even considered early on, but now it is the most pervasive, single biggest concern.
2. *Be certain of the problem you are trying to solve*. Holmes advised to analyze the specific problem because it may differ in practical reality from a general characterization of the issue.
3. *Examine what others are doing*. In many cases, someone else has already confronted similar problems. Holmes recommended that security managers reach out to others in the same industry to find solutions and shamelessly steal good ideas.
4. *Use the correct tool for the job*. Sometimes the best solution is not technical. Changes to processes and procedures sometimes solve a problem without any procurement of equipment. Technology is best used to increase the effectiveness of the humans operating the system rather than as a solution in itself, a so-called silver bullet.

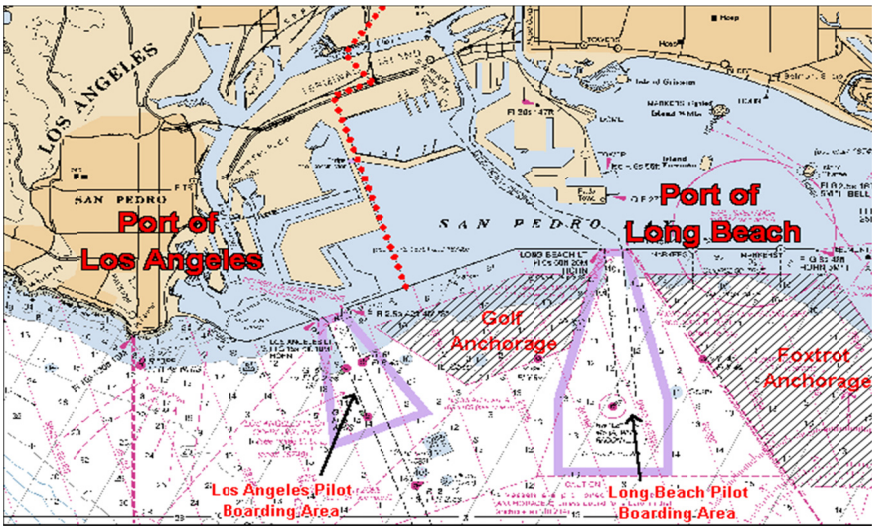

FIGURE 3-3 Maritime Domain Awareness is as much about processes and procedures as it is about technology; it is a merger of high-tech with low-tech; it is the ultimate exercise in information fusion; when successful, it is a powerful tool to prevent and/or deter incidents; it pays dividends in other areas. SOURCE: National Oceanic and Atompheric Administration. Available at: http://www.ioos.noaa.gov/global/geo_global_hfr_mar2012.pdf; accessed October 9, 2014.

5. *When you think that you have the right solution, check it again*. An independent analysis of the solution brings a fresh perspective that can find flaws in reasoning or fact that can save millions of dollars.
6. *Conduct a thorough cost analysis*. If the cost analysis is incomplete or inaccurate, the security manager may commit the organization to unexpected costs, sometimes extending years into the future.
7. *Don't overbuy or overcomplicate the project*. Unnecessary complexity in a security system is usually a liability rather than an asset. Solutions that are easier to instill, maintain, and repair are generally more sustainable.
8. *Strive for compatibility*. One cannot just redesign the overall system. Work with the existing system, and at times, practical considerations irrelevant to security can override an ideal solution. A sophisticated component or system that does not integrate well with the larger system generally does not deliver the capability that justified the sophistication. Also, implementing security systems takes time, and in many cases the technology will need to be updated even before completion of the implementation, so standardization and compatibility are important.

9. *Coordination and cooperation are critical*. Even a huge port is only part of a larger system. Having a high-level plan and a mechanism to coordinate implementation of that plan minimizes unnecessary arguments and unproductive conflicting efforts within and across organizations.
10. *Focus on prevention*. Prevention of an incident is the most important effort. Learning from an event and focusing on how to prevent the next one is a better use of time and effort than figuring out how to improve response.

In parting thoughts, Holmes noted that the perfect can sometimes be the enemy of the good: a basic system that works is better than an ambitious security system that does not operate. This is also true of Maritime Domain Awareness (MDA) as described in Figure 3-3. He said that training is important because those who operate the systems on a daily basis are key to the effective operation of the overall system. They should understand how their jobs affect overall security. Finally, he reiterated that honest assessments of failures are critical to improving security.

4

Science and Technology to Counter Terrorism in Critical Areas

CYBERSECURITY IN ITS COMPLEXITY

Understanding Cybersecurity and Related Challenges

Srinivas Mukkamala opened his presentation by stating that cybersecurity issues appear to be simple, but are actually very complex. The vulnerabilities associated with many of our cybersystems arise whenever newer sub-systems are integrated with existing, outdated systems. This has become a serious problem particularly in protecting critical infrastructures in the United States. One example Mukkamala raised was that of the many computerized systems in hospitals. If these systems were compromised, patients' health could be seriously threatened. Mukkamala and his colleagues concluded that Level I trauma centers are vulnerable, due to systems that have minimal or in some cases no security features.

Mukkamala then described the international online marketplace for exploits and personal information. There are individuals and illicit businesses whose business model is to sell the capability to exploit software vulnerabilities in other people's computer systems and enable the purchaser to misuse the information or the system. There are websites where these exploits are marketed and sold among trusted users.

Similarly, personal and credit card information are bought and sold, enabling identity theft around the world. An identity is easy to steal, and such theft is very serious for those who are victimized. The information is often acquired illegally by malware that enables hackers to gain access to individuals' computers or to databases of thousands or millions of people.

Unfortunately, antivirus software does not detect malware. It can look for anomalies and known exploits, but new malware can go undetected. Malware trees can be constructed showing the relationship among different types of malware and the methods they use. These can be useful in forensics on a cybersecurity event, but they fall short of attribution. In Mukkamala's view, the largest problem in addressing cybersecurity is the lack of reliable attribution methods. As a result, those who seek to commit a crime or an act of terrorism via cyberspace can be reasonably sure that they will not be detected and quite confident that they will not be identified.

Similarly, insider threats are a serious problem because it is difficult to detect a breach of cybersecurity, and when it is detected, it is not easy to identify the culprit(s). In particular, privileged users, such as system administrators, can move through systems without tracking.

The Department of Homeland Security (DHS) in the United States has therefore recommended that every 72 hours all critical infrastructure systems should be scanned for unusual or nefarious activity. A key to success is cyberthreat intelligence, so timely sharing of information is essential.

Cybersecurity Challenges in India

B. J. Srinath spoke about cybersecurity concerns in India and the efforts taken by the government to regulate and address the problem. He stated that cybersecurity threats are global and require cooperation across nations. The government of India cooperates internationally, including conducting joint exercises with the United States Computer Emergency Readiness Team (US-CERT). Cyberthreats have increased in sophistication, both by criminals and by governments. Many countries are developing capabilities for cybersurveillance and cyberattack. Malware from these different sources is now targeting mobile devices in addition to networked computers. The government of India has been working through public-private partnerships to tackle some of the problems related to cybersecurity. Due to concerns regarding loss of reputation and the need to protect proprietary information, many commercial organizations do not report cybersecurity incidents.

Srinath concluded by stating that a large number of cyberattacks take the form of the hacking of websites to proliferate political views, often views that are violent or may incite violence.

DISCUSSION

R. Narasimha began the discussion by stating that according to press reports a significant number of financial cyberattacks are conducted in India, or that those who conduct the attacks are being trained in India. **N. Balakrishnan** replied that cyberthreats at Indian banks are treated as pollution. India is a source of a significant amount of spam and it also has a large number of botnets, which may be used in an attack, but India is not the source of attacks. A participant asked if there are efforts parallel to those in the life sciences to establish norms of behavior. Mukkamala noted that in some countries cyberattacks are not illegal and in others, such as Germany, selling exploits is legal. Another participant pointed out that purchasing such exploits is how companies like Microsoft discover and fix security problems in their own software. With regard to credit card fraud, India does not have any legal requirements to disclose or even report the number of credit cards compromised, for example. The only requirement is that the incident be reported to CERT. Cyberspace today suffers from underreg-

ulation rather than over regulation, added Srinath. Further, laws and regulations vary greatly across different countries, which makes tracking crime difficult.

Another participant noted that automated cybersecurity threats also exist. Balakrishnan stated that 20 percent of tweets are machine originated, which enables the amplification of a message or the spread of a potentially dangerous message. In India, the use of websites, social media, and other cyber means to recruit terrorists, incite terrorist acts, and even coordinate activities is a real concern.

Other issues were raised by workshop participants. One participant asked if it was possible for hackers to hack into air traffic control systems to bring down a plane. Srinath stated that he believed it was just a matter of time before these types of security breaches would occur. Although some such systems are air gapped (have no direct connectivity to other information systems), "an air gap is no air gap." At some point the gaps are breached through error (unwitting file transfers) or deliberately.

Finally, **Van Romero** proposed a prioritization approach. A simple penetration does not constitute a significant compromise of valuable information or loss of control. Banks, like vegetable sellers, assume some loss. They protect the important parts and do not worry much about the rest. One has to factor in some threats and security breaches, but critical assets should be protected.

GLOBAL HEALTH SECURITY AND STRENGTHENING PUBLIC HEALTH INFRASTRUCTURES

The Anthrax Letters: Lessons for Leaders

David Franz began by noting that he would discuss the anthrax letters that were sent to politicians and prominent members of the media in October 2001, and his underlying approach is preserving the good of powerful science in a dangerous world.

Franz first provided a very brief overview of biology in the 21st century and a short history of safety and security. He then discussed the anthrax letters, but brought in two other cases that he considers insider issues, although they are not as well known as the anthrax letters. Franz then turned to the U.S. government response and the implications of the government's response for the life sciences enterprise. Finally, he briefly discussed what leaders can learn from all of this and how we can find a balance in the way we respond to these types of incidents. Franz explicitly did not discuss the technical, forensic, or other issues related to the anthrax letters. Franz quoted from the U.S. National Academy of Sciences' (NAS) report that examined technical issues regarding the anthrax letters and the investigation and forensics that followed.[1] One relates directly to the idea of the insider threat. It says, "An unavoidable observation from the

[1]National Academy of Sciences. *Review of the Scientific Approaches Used During the FBI's Investigation of the 2001 Anthrax Letters*. Washington, D.C.: The National Academies Press, 2011.

2001 *Bacillus anthracis* mailings is that the best subject matter experts in a given area might also be viewed as suspects."[2] The report's highest-level summary conclusion was, "It is not possible to reach a definitive conclusion about the origins of the *B. anthracis* in the mailings based on the available scientific evidence alone."[3] Franz recommended the report to anyone interested in the technical, law enforcement, and forensic response.

Where does bioterrorism or the insider threat fit into the whole spectrum of terrorism problems addressed at this workshop? The anthrax letters killed five people.[4] Atomic bombs dropped on Japan during World War II killed an estimated 250,000 people.[5] Experts believe that about 10,000,000 to several million people died worldwide in the 1918 flu pandemic.[6] Another data point on a potential scale is the 1965 New York City subway trial in which researchers released a simulant of anthrax.[7] They estimated that in one day approximately a million people could be infected with anthrax spores.[8] Fortunately, there have not been any intentional, high-impact events. In thinking through how to scope the bioterrorism prospect, Franz referred to John Vitko, who led the biosecurity program at DHS in the science and technology (S&T) directorate. Vitko coined what he called a "Vitko unit": If an event kills 10,000 people or costs $1 million, that is one Vitko unit, and any event above that unit, he believed, should be addressed by DHS S&T (see Figure 4-1). This is just one example of how one person tried to deal with a very complex problem with a lot of unknowns.

Franz turned very briefly to 21st century biology, which has undergone a revolution in the last 20 years. Genes from different organisms can be spliced together to make new organisms and new organisms can be designed from scratch. The rate at which base pairs can be sequenced is rising faster than the increase in microprocessor speed resulting from the increase in the number of

[2]Ibid, p. xvii.

[3]Ibid, pp. 4, 118.

[4]Ibid, p. 44.

[5]Bernstein, B. J. "The Atomic Bombings Reconsidered." *Foreign Affairs*, Jan./Feb. 1995. Available at: http://www.foreignaffairs.com/articles/50569/barton-j-bernstein/the-atomic-bombings-reconsideredhttp://www.foreignaffairs.com/articles/50569/barton-j-bernstein/the-atomic-bombings-reconsidered; accessed September 22, 2014.

[6]Taubenberger, Jeffrey K. and David M. Morens. "1918 Influenza: the Mother of all Pandemics." *Emerging Infectious Diseases*. Vol. 12, No. 1. January 2006. Available at: http://wwwnc.cdc.gov/eid/article/12/1/pdfs/05-0979.pdf; accessed October 20, 2014.

[7]These simulations were conducted when the United States had an offensive biological warfare program until 1969, when it was stopped by President Richard Nixon.

[8]Gerstein, D. *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*. Annapolis, MD: Naval Institute Press, 2009, p. 68. Available at: http://books.google.com/books?id=JbJOuG4Q3_IC&pg=PA1&source=gbs_toc_r&cad=3#v=onepage&q=1966%20New%20York%20subway&f=false; accessed Sept. 22, 2014.

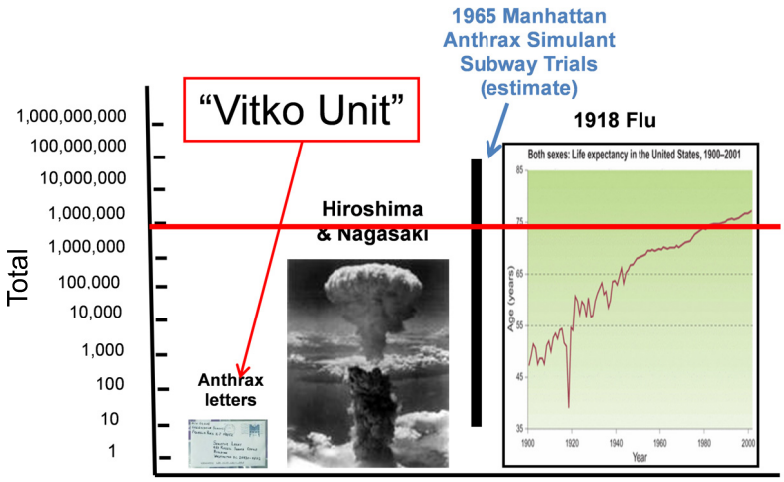

FIGURE 4-1 John Vitko coined what he called a "Vitko unit." If an event kills 10,000 people or costs $1 million, that is one Vitko unit, and any event above that unit should be addressed by the Department of Homeland Security, Science and Technology Directorate. NOTE: The 1918 flu graph contained within this figure is set to the height of the "y" axis of the larger figure. SOURCE: Franz, 2014.

transistors that can be fit on a semiconductor chip (the Carlson Curve rises faster than Moore's Law). This is a revolution, and it is not only occurring in India or in the United States. It is global. Franz stated that proliferation of technologies, proliferation of knowledge in biology, is essentially over. Proliferation of tacit knowledge, how one cooks the recipes, may not be over. The proliferation of this knowledge is a global issue.

Franz said that when he was on active duty as late as 1998, the focus was on safety, and there was little talk of biological security. In his command brief in 1997, Franz said his three top priorities, in addition to providing medical countermeasures for the war fighter, were safety, safety, and safety because people were working in biosafety level (BSL) four labs with hemorrhagic fever viruses. One needle stick or one bone fragment through a glove could be almost certain death. He wanted to get as close to a zero-defects operation as possible. Much of those safety practices came from the former offensive program in the United States. Arnold G. Wedum, a physician at Fort Detrick in the 1950s and 1960s, developed what eventually became the first section of the Centers for Disease Control and Prevention (CDC) guidelines. After the turn of the 21st century, a series of events (September 11, 2001 [9/11] and the anthrax letters, which Franz calls 10/4), caused the science community, in this case represented by NAS, to start thinking about becoming involved in these issues.

Right before these incidents, there was a surprise in biology in Australia with an ectromelia virus, a mousepox virus. Then there was de novo synthesis of

polio; this was the second time it was done by E. Wimmer.[9] This was followed by a surprise in something learned about orthopox viruses called a spice gene that was a virulence factor. All of these discoveries, along with the biotech revolution, were accompanied by an incredible budget increase in the United States for biosecurity, which went from $137 million in 1997, most of it allocated to the Department of Defense (DOD), to $6 billion in 2002.

NAS assessed this situation and formed a committee chaired by Gerry Fink from Massachusetts Institute of Technology. Franz served on that committee, which wrote a report titled *Biotechnology in the Age of Terrorism: Confronting the Dual Use Dilemma.*[10] The committee concluded that life science research underpins so many elements that are critical for health, food, energy, security, and for all of us. However, good science can be put to bad uses. It may be unlikely; maybe it will not occur very often, but these are very powerful tools that could potentially be put to bad uses. The report recommends education and awareness as the key ways to address this potential threat. The report also recommended that the U.S. government form a high-level committee in the Department of Health and Human Services—not in a security agency—that would bring together security professionals and health professionals for the first time. This was called the National Science Advisory Board for Biosecurity (NSABB).

When Franz awoke on the morning of August 2, 2008, a picture of his previous laboratory and Bruce Ivins, one of the scientists in that laboratory, was being shown in the media. Ivins was a Federal Bureau of Investigation (FBI) suspect in the anthrax letters case, and he had just committed suicide. Franz recounted that he was giving a talk shortly thereafter, and he had first made a slide that said "the insider threat is more *serious* than I thought," but he quickly changed that slide to read, "the insider threat is more *difficult* than I thought." The insider threat is a really tough challenge. As Joshua Lederberg said about biological warfare in general, there is no technical solution to this problem. It will require an ethical or a moral solution.[11] Then he paused and asked, would an ethical or moral solution appeal to a sociopath? Franz believes that encapsulates some of these issues that we are dealing with not only in regard to biology, but also in other fields as well.

Within 4 days of Ivins' death, Congress responded. Two congressmen wrote a letter to President George W. Bush stating that if the allegations are true, the FBI has identified a serious weakness in security at one of the nation's prem-

[9]Molla, A., et al. "Cell-Free, de novo Synthesis of Poliovirus." Available at: http://www.ncbi.nlm.nih.gov/pubmed/1661029; accessed October 20, 2014.

[10]National Research Council. Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology. *Biotechnology Research in an Age of Terrorism*. Washington, D.C.: The National Academies Press, 2004.

[11]Preston R. "Annals of Warfare: The Bioweaponeers." *The New Yorker*, March 9, 1998, pp. 52–65. Available at: http://www.newyorker.com/magazine/1998/03/09/the-bioweaponeers; accessed September 26, 2014.

ier laboratories for the study of some of the most deadly pathogens in the world. Their allegations also raised equally troubling security concerns about thousands of other scientists and technicians who work with select agents in hundreds of labs across our country. The same year the Graham-Talent Commission wrote a report called *World at Risk*.[12] Suddenly biology was elevated to a significant risk, but the commission also said the United States should be less concerned that terrorists will become biologists and far more concerned that biologists will become terrorists. This report is referring to experts like those gathered at the workshop. Shortly thereafter, DOD implemented a new regulation called AR50-1 that has been used in draft form since 2004, called Biological Surety.[13] Those who have worked in nuclear programs know nuclear surety very well. Franz had worked in a chemical program at the U.S. Army Edgewood Chemical Biological Center where there was a chemical surety program. Biology, however, had never had a surety program of this kind. The surety program includes not only safety, which biologists in a lab like Franz's know and love and appreciate and support, but also security. Biologists do not mind fences around the labs, or cameras in their labs. That really does not bother them. An agent accountability program was also introduced and it quickly fell apart because it is very hard to know how to account for replicating agents that are hard to measure. Therefore, that program was ended. It is easier to account for chemicals and radiological and nuclear materials than for some biological agents.

There is also a personnel reliability program that is meant to address questions such as: Are scientists mentally alert, emotionally stable, trustworthy, and so on? Franz highlighted a couple of lines from the AR50-1 that hint at what the certifying official should look for in an employee: inappropriate attitude, negligence, delinquency, arrogance, flippancy, and so on. Someone sent Franz a blog written about the time this list came out and the person said, "this reminds me of many scientists I know." Really smart people are often just a tiny bit weird and quirky, and often irritating. Again, this describes experts like us. Interestingly, DOD did implement the program, which was signed on July 28, 2008. Bruce Ivins died at his own hands on July 29, 2008, although the program had been in place in the lab at which he worked for some time.

In addition to the issues associated with Ivins and the anthrax letters, another recent set of events has shaped thinking and practice regarding biosecurity in the United States.

---

[12]Graham, B., and Talent J. *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*. New York: Random House, 2008.

[13]Department of the Army. Army Regulation 50-1. "Nuclear and Chemical Weapons and Materiel, Biological Surety." Washington, D.C., July 8, 2008. Available at: http://fas.org/programs/bio/resource/documents/biological_surety_08.pdf; accessed September 22, 2014.

The United States National Institutes of Health National Institute for Allergy and Infectious Diseases (NIH NIAID) funded two scientists to take the H5N1 virus and try to make it transmissible in mammals. There has been a pandemic of H1N1, which transmits very easily between humans, but it is not too virulent and it does not kill many people. H5N1 does not transmit easily between humans. It transmits from a chicken to a human, or a duck to a human, or a wild bird to a human, and perhaps 60 percent of the cases are lethal. NIH therefore asked two scientists, one in Rotterdam and one at the University of Wisconsin (Fouchier and Kawaoka, respectively), to take the H5N1, mutate it, and produce a virus that was transmissible by air in ferrets, which is the best flu animal model. The researchers succeeded. They did exactly what they were asked to do, but one of them, Ron Fouchier, started making statements.[14]

First, in Malta, he said that this is very bad news, and then he said this flu is as efficiently transmitted as seasonal flu, and then in an interview he said that it is probably one of the most dangerous viruses one can make. Then both Fouchier and Kawaoka submitted their papers to *Science* and *Nature*. Those journals brought the articles to NSABB, which read them and determined that there were elements of the papers that should not be published, such as the gene sequences and the approximately five to seven mutations. NSABB also recommended that the international community be involved. The U.S. government and Tony Fauci, director of NIAID, led this effort. A meeting was organized with the World Health Organization (WHO) that brought representatives of 13 or 14 other countries to discuss this issue. At that meeting, Fouchier presented slightly different data, and the WHO meeting concluded with a statement that the data should be published. Then NSABB examined the issue again in March 2012, and voted unanimously that Yoshi Kawaoka's paper should be published, and voted 12 to 7 that Fouchier's should be published, and they were subsequently published.[15]

Franz does not consider this episode a technical surprise. If anything, he considers it an ethical lapse on the part of a scientist, a legitimate scientist, who was not trying to do harm, but some of his statements caused issues that were uncomfortable for a number of people. Shortly thereafter, another new guideline was released by NIH, which must be followed by those who wish to receive funding from NIH: the framework for guiding the U.S. Department of Health and Human Services funding decisions regarding highly pathogenic H5N1

[14]Fouchier, R., et al. "Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets." *Science*, June 22, 2012, vol. 336, no. 6088, pp. 1534-1541. doi: 10.1126/science.1213362. Available at: http://www.sciencemag.org/content/336/6088/1534.full; accessed September 21, 2014. See also Harmon, K. "What Will the Next Influenza Pandemic Look Like?" *Scientific American*, September 19, 2011. Available at: http://www.scientificamerican.com/article/next-influenza-pandemic/; accessed September 21, 2014.

[15]National Science Advisory Board for Biosecurity. Findings and Recommendations, March 29-30, 2012. Available at: http://osp.od.nih.gov/sites/default/files/resources/03302012_NSABB_Recommendations.pdf; accessed September 22, 2014.

"gain-of-function research."[16] This refers to research that changes a virus's virulence, for example. In this set of guidelines, two issues were addressed. First, one should not do anything that nature is not going to do in the future. But discerning what nature will do is difficult. Second, one has to assure that biosecurity risks can be sufficiently mitigated and managed. Franz stated that he did not know how to do that either. He knows how to mitigate and manage biosafety risks, but it is not clear how to mitigate and manage biosecurity risks. The guidelines were published in February 2013.[17]

There are three individuals whose cases have led to biosecurity measures in the United States. The first one was Larry Wayne Harris, who tried to acquire plague bacillus in 1996 from the American Type Culture Collection.[18] This is a center in Virginia near Washington, D.C., where isolates of many bacteria and viruses are kept for scientists to use. He tried to acquire it illicitly by forging stationery and stating that he had a clinical laboratory. This incident led to the select agent rule that states that if two laboratories want to exchange a select agent, both laboratories must be certified by the CDC. Next, after the anthrax letters, army regulations as well as the USA Patriot Act were adopted.[19] The USA Patriot Act changed the select agent rule by registering scientists who work with select agents, not labs. Finally, after the H5N1 issues, there is a new policy or regulation on oversight of life sciences dual-use research. Three individuals who did something either illegal or possibly unethical had a significant impact on the regulatory scheme that scientists are now living with in the life sciences enterprise.

Franz provided additional examples of how hard this problem is to address. For the years 2009 and 2010, Gigi Kwik Gronvall and her colleagues at the University of Pittsburgh Medical Center identified naturally occurring outbreaks of select agents.[20] They are everywhere, obliterating her map. Another very specific example is of Supaporn Wacharapluesadee, a researcher from

[16]National Institutes of Health. "A Framework for Guiding U.S. Department of Health and Human Services Funding Decisions about Research Proposals with the Potential for Generating Highly Pathogenic Avian Influenza H5N1 Viruses that are Transmissible among Mammals by Respiratory Droplets." February 21, 2013, p. 2. Available at: http://osp.od.nih.gov/sites/default/files/funding-hpai-h5n1.pdf; accessed September 18, 2014.

[17]National Institutes of Health. "A Framework for Guiding U.S. Department of Health and Human Services Funding Decisions," February 21, 2013.

[18]See, for example, Revkin, A. "Arrests Reveal Threat of Biological Weapons." *New York Times*, February 21, 1998. Available at http://www.nytimes.com/1998/02/21/us/arrests-reveal-threat-of-biological-weapons.html; accessed September 18, 2014.

[19]U.S. Congress. H.R. 3162. Patriot Act. Available at: http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf; accessed October 24, 2014.

[20]Center for Biosecurity. *Everywhere You Look: Select Agent Pathogens.Countries in which naturally occurring disease outbreaks caused by select agent pathogens were observed, January 1, 2009 through October 31, 2010*. Available at http://www.upmchealthsecurity.org/diseasemap/index.html; accessed September 21, 2014.

Chulalongkorn University in Bangkok.[21] She studies an emerging disease, the Nipah virus, which killed many pigs and some people in Malaysia. All she does is lay plastic tablecloths under fruit bat roosts, collects the bat droppings, and isolates the virus from the bats fairly easily. The ease with which she and others can conduct this research demonstrates that it is not possible to lock up the bugs.

Franz's concern is the over-regulation of the life sciences. A balance between research and security has to be found. Regulations are needed, but there has to be a balance with the conduct of science. Franz is concerned that overregulation will affect our ability to provide health care, food, agriculture, and energy. It will affect the economy, the ability to compete globally, and even national security. It may take 5 to 10 years to know the full effect of overregulation on the life sciences and then maybe to rebuild and turn the trend around.

What can we do? Franz asked. We cannot lock up the bugs. We cannot control equipment and technology. We have tried on an international scale to do this with mechanisms like the Australia list. We cannot control knowledge. We cannot isolate scientists. We cannot know all the biohackers that might be out there. What we can do is to build awareness and understanding. We have tried that, and Franz thinks it has been pretty successful, even globally. We can seek to communicate and build trust in laboratories and globally, and Franz does not think we have tried hard enough in that area. We can use good to counter harm, technologies to produce medical countermeasures and other discoveries; we have been semisuccessful there. We can apply leadership principles in labs. In the United States, we have not tried hard enough to do this. We can impact the culture of laboratories, especially our biological security laboratories. With regard to the way ahead, the life sciences community needs to take an active role, to take responsibility and not just sit back. There needs to be transparency in science. Scientists need to communicate with, educate, and recruit young scientists. They need to demonstrate a culture of responsibility and build public trust, build communities of trust, and work with regulators. We need some regulation, but we need to consider the real risks, consider the real safety or security that we gain from a given regulation and think this through very carefully, and consider the entire cost because there are always tangible and intangible costs when implementing regulations. One of Franz's philosophies when he was commanding the U.S. Army Medical Research Institute for Infectious Diseases was to seek solutions that limit the frustration of scientists, because 99.9 percent of the scientists just want to work hard and do a good job. If one overlays or hampers the ability of scientists to do their work just because there might be an outlier within that group, the approach may be out of balance.

[21]Wacharapluesadee, Supaporn, et al. "Bat Nipah Virus, Thailand." *Emerging Infectious Diseases*. Vol. 12, No. 1, January 2006. Available at: http://wwwnc.cdc.gov/eid/article/11/12/pdfs/05-0613.pdf; accessed October 20, 2014.

With regard to communities of trust, Kendall Hoyt at Dartmouth College, who wrote a book called *Long Shot: Vaccines for National Defense,*[22] examined why the U.S. government was able to produce defense vaccines in the 1940s, 1950s, and 1960s, and why we just cannot seem to deliver them to soldiers or citizens today, although technologies are better and regulatory schemes are a little bit higher. She reached two conclusions. One, in those days, there was a champion who would take that antigen all the way from its technological base through animal testing, and stick with it and fight for that antigen as he or she developed a vaccine. The other conclusion was the existence of communities of trust. There were individuals that came out of World War II who worked at Walter Reed Army Institute of Research. Maurice Hilleman, for example, who was on many NAS committees, went to work at Merck. Someone else went to Pfizer, and Maurice would call his friend at Pfizer and ask: What was that cell line we used at RARE when we were making that vaccine? The person at Pfizer would actually tell him. Now there are rows of lawyers standing between the scientists. Those communities of trust, Hoyt found, were critically important in making progress. A high-trust organization increased value, accelerated growth, enhanced innovation, improved collaboration, strengthened partnership, improved execution, and heightened loyalty. Low-trust organizations have redundancy, bureaucracy, politics, disengagement, turnover, and fraud. As leaders in our organizations, Franz said, we can move our organizations to become high-trust organizations. Enlightened leaders who lead with science, talk about quality, and emphasize safety, vision, education, and so on, can make a difference in the cultures of organizations. This is hard to do, and it does not scale easily. It is much easier to put a fence around something than to find a leader who does a great job.

Of the many risks and threats, Franz is actually more concerned about chronic diseases, communicable diseases, and emerging diseases, but we may also have lab accidents. We may have intentional misuse of information. We may have bioterrorism. We may even have biowarfare by nation-states. However, Franz said, our approach needs to be balanced. We cannot just regulate these potential threats away. We need enlightened leadership, a culture of personal and corporate responsibility, and leaders who are willing to take responsibility to develop thoughtful regulation and safe and sustainable practices, and maintain freedom for scientists to explore so that we can make progress for all people in the life sciences.

Franz concluded that there is only one way to entirely eliminate risk: that is to turn out the lights, unplug the freezers, board up the doors, send everyone home, and let weeds grow in the parking lot of laboratories. There would be no more insider risks; however, there would also be no more science. As a result, we cannot afford to have zero risk. It is just not an option. It is a dangerous

[22]Hoyt, K. *Long Shot. Vaccines for National Defense*. Cambridge, MA: Harvard University Press, 2012.

world and we must work through these issues together. It is very important to work together globally because what happens in one country impacts another.[23]

Global Health Security in India: India's Experience with H1N1

J. K. Bansal began by stating that in the last decade, several pathogens have emerged, causing infectious diseases such as Chikungunya, dengue fever, severe acute respiratory syndrome, Japanese encephalitis, Congo-Crimean hemorrhagic fever, H1N1, and H5N1. In addition, there are reports that terrorist organizations are attempting to acquire biological agents such as anthrax, plague, and smallpox; possible sources of these agents could be a microbiology lab, a veterinary lab, or a facility associated with the biotech industry. However, as of today, the emphasis is on biological terrorism because biological weapons are relatively cheap and easy to produce, and a very small amount that can cause havoc. Terrorists could also use a genetically modified organism, which is difficult to detect. There are no vaccines, drugs, or antibiotics available to treat some of these diseases. Some of these agents, specifically anthrax, can be manufactured in a very crude, improvised laboratory and can be disseminated relatively easily.

Therefore, it is important to have biosafety measures and, specifically, biosecurity measures. The National Disaster Management Authority (NDMA) of the government of India, where Bansal is a member of the leadership, is deeply concerned about bioterrorism and has formulated national guidelines for biological disaster management, including bioterrorism. These guidelines cover biosafety, biosecurity, management of epidemics and pandemics, countermeasures for bioterrorism, management of animal disease, and agroterrorism. On April 21 and 22, 2008, NDMA organized a conference entitled, "A National Workshop on Pandemic Preparedness: Beyond Health." The information exchanged at the conference and captured in the proceedings proved to be helpful in preparing business contingency plans in nonhealth sectors with topics including:

- Supply of food and essential commodities
- Water resources
- Law and order
- Transportation – surface transport and shipping
- Transportation – civil aviation
- Transportation – railways
- Information and communication
- Power

[23]Franz, D. "The Dual Use Dilemma: Crying Out for Leadership." *Saint Louis University Journal of Health and Law Policy*, Vol. 7, Issue 1, 2013. Available at: http://www.slu.edu/Documents/law/SLUJHP/Archives/Vol7-1/Franz_Article.pdf; accessed September 22, 2014.

- Commerce and industry
- Rural sector needs
- Finance
- Defense

Further, a steering group on global health security held a meeting in June 2013 at Chatham House.[24] As a member of that group, Bansal presented on India's multisectoral approach, and his paper was subsequently added to the document of the meeting. Participants agreed on the need for a whole-of-government approach, similar to what NDMA planning in India stresses: an approach that includes not only the public health sector and law enforcement, but also water, transportation, telecommunications, and energy sectors. The participants agreed on a common framework for global health security, which included prevention, detection, and rapid response to infectious diseases of international concern. Specifically, the steering group recommended global health security first by focusing on prevention by promoting biosafety and biosecurity. Measures suggested include the control of infectious disease outbreaks and the prevention of emergence of drug-resistant microorganisms. The second set of recommendations focused on early detection through biosurveillance and by developing laboratories capable of accurately detecting a biological agent and reporting biological incidents or biothreats of international concern. The third set of recommendations focused on rapid response by developing mechanisms for multisector response.

As an overview of global health security in India, Bansal listed the primary organizations and agencies involved: NDMA, National Crisis Management Group, Ministry of Health and Family Welfare, State and District Health Department, Primary Health Care System, government and private medical institutions, research institutes such as the Indian Council of Medical research, Defense Research Development Organization, and agencies related to the health care sectors such as those involved with water supply, hygiene, and international organizations.

For early detection of an infectious disease, India has initiated a project called the Integrated Disease Surveillance Program (IDSP). IDSP organizes structures at the national level, state and district levels.

If a dangerous pathogen emerges, it is immediately reported for a prompt response. Weekly information is provided by program offices of district surveillance units and on to regional surveillance units and then to state surveillance

[24]The Chatham House Steering Group held a meeting in June 2013 on Global Health Security, and recommended the prevention of avoidable epidemics by promoting national biosafety and biosecurity systems, detecting threats early through biosurveillance, rapid response, and establishing a multi-sectoral response capacity to effectively counter biological threats of international concern. Global health security risks are considered multinational pandemics, which require international cooperation such as on global disease surveillance, airport quarantines, and other measures.

units. This information is obtained from the peripheral health systems, for example, a primary health care center, a district hospital, or a private practitioner. With regard to biosurveillance, the Indian government has worked with the BSL-4 laboratory in Pune and there have been proposals for a BSL-3 laboratory as well. Some of the biological agents, such as anthrax, are especially dangerous because in the powder form it can be sustained for a longer period and disseminated through a central air conditioning system reaching any part of a building. Therefore, sensitive buildings, such as airports, hospitals, and railway stations, need to be protected by lighting, grill work, intrusion alarms, and increased surveillance.

During the Commonwealth Games held in India in 2010, a foolproof security system for chemical, biological, radiological, and nuclear (CBRN) threats was put in place, Bansal said. For biological agents, they have initiated a biological standard for detector systems that can sense a biological agent at a distance of up to 5 kilometers. The integrated biological disease detection system is very useful for field purposes and can detect and respond to incidents. Planning needs to be done before an event, during an event, and after an event. Key elements of planning include intelligence before an event; detection, protection, and decontamination at the time of an incident; and further investigation after an incident. For response to a suspected bioterrorist attack, individuals or victims would be hospitalized first and then a message would be sent to the director of emergency response, who in turn would inform the Ministry of Health and Family Welfare, and sends a rapid response team for investigation, containment, and other tasks. The Ministry of Health and Family Welfare then would request the involvement of the Ministry of Defense. In the event of an incident, the Ministry of Defense's medical services would reinforce the response teams, and military hospitals would be ordered to admit patients.

International cooperation is also very important. In the 21st century, disease outbreaks in one country can be disseminated to other countries through rapid transportation. Due to incubation periods, which for anthrax may be 4 to 6 weeks, an infected person may not feel or appear sick for some time; however, during that period, an individual may infect others. Therefore, it is very important to screen passengers coming from a country where a particular disease is prevalent. Similarly, if a particular country has a high prevalence of an infectious disease, screening prior to passengers departing can prevent further infections. For example, more than 120,000 migrant workers from India went to Saudi Arabia. India deploys trained medical teams at the airport to screen returning passengers for those with symptoms of Middle East respiratory syndrome coronavirus.

International cooperation is essential for these and a variety of initiatives. Bansal offered several suggestions, beginning with broader adoption of the 2005 International Health Regulations. He then proposed a web-based forum where the scientists and experts could interact with each other to formulate strategies on how to combat or counter biothreats. He suggested a stockpile of various antibiotics and vaccines at regional levels. In terms of research, Bansal under-

scored the need for joint cooperation on the most dangerous diseases. Joint exercises, he said, should be conducted to develop communication systems and on-the-ground coordination between countries prior to an incident because such cooperation in the midst of a response is not possible. Pooling medical expertise and resources and exchanging ideas and best practices can also improve the management of pandemics and other types of incidents.

India has taken the initiative in advancing international collaboration. There are cooperative programs with CDC in Atlanta, including one on the detection and prevention of emerging pathogens. In May 2013, a joint conference on the emergence and reemergence of pathogens and biorisk management was organized by NDMA in collaboration with CDC.[25] Decision makers at the highest levels also participated, because the conclusions and recommendations of any meeting or conference must be implemented to be effective. In 2007, India participated in an Interpol conference on biosafety and biosecurity.[26] In February 2012, India hosted a meeting of the South Asian Forum for Health Research, where delegates participated from a variety of countries, including Bangladesh, Bhutan, Malta, Nepal, Pakistan, and Thailand.[27] Meeting participants deliberated transmission of a variety of infections and implementation of countermeasures. NDMA also organized a meeting with the World Society for the Protection of Animals, during which animal diseases and zoonotic diseases were discussed in detail.

Bansal then turned to India's experience with managing H1N1. NDMA took proactive measures, applying lessons learned from the avian flu outbreak in 1918, which killed one-third of the population.[28] As early as April 2009, the

[25]A two-day conference was held exclusively on "Emerging and Re-emerging Pathogens & Bio–risk Management" on May 7 and 8, 2013, in Delhi to develop best practices to deal with effective prevention and mitigation of biothreats. Renowned experts in biodefense from India and the United States participated to draw a roadmap for prevention, mitigation and preparedness.

[26]An Interpol workshop on preventing bioterrorism was held in Muscat, Sultanate of Oman, March 19-21, 2007. It was attended by 62 delegates from 15 countries, including senior police officers, government representatives, and representatives of the health, scientific, and academic communities. The objectives of workshop were to provide information and training, to encourage the development of a response capability, to promote relations between and with regional, national and international organizations, and law enforcement agencies, to develop a draft plan of action on a regional, national and international basis, and to present the Bioterrorism Incident Pre-planning and Response Guide.

[27]India is the chair of Asian Regional Health Forum. In February 2012, India hosted the 4th meeting of the Forum. Delegates from Bangladesh, Bhutan, Maldives, Nepal, Pakistan, Srilanka, Thailand and India participated. Cross border transmission of infections in neighboring countries and counter measures were discussed.

[28]Lessons learned from the 1918 avian flu pandemic were discussed, including both health and non-health emergency areas. Necessary business continuity planning of essen-

H1N1 pandemic alert was sounded by WHO. India initiated a prompt and effective response.[29] Kits and personal protective equipment were distributed at airports and passengers were screened. The personal protective equipment, kits, and nasopharyngeal swab kits were also made available at hospitals designated to treat H1N1 in major cities such as Bangalore, Delhi, Hyderabad, and Pune. These hospitals had diagnostic kits, medicines, isolation wards, and quarantine facilities. NDMA, along with the Ministry of Health and Family Welfare, began screening passengers arriving from affected countries. Pharmaceutical companies were instructed to enhance their manufacturing capacity for Tamiflu should greater supply be required. Community awareness involved the regular dissemination of what should and should not be done to avoid concern or panic.

A control room was established at airports and in state crisis management groups. These control rooms were in constant contact with NDMA, the National Crisis Management Committee, and district authorities. Business community plans and in non-health-sector plans were also prepared.

For pandemic response, three points were adopted: (1) medical intervention with antiviral drugs, vaccines, and medical care; (2) nonmedical intervention through personal hygiene, and quarantines; and (3) food, power, transportation, and telecommunications. There was a contingency plan for maintaining the essential services of food, water, and health care. A multisectoral approach was adopted involving the health, defense, finance, transport, and telecommunications sectors. Through this methodology and a proactive approach, India experienced only minimal impact from H1N1. The Ministry of Health and Family Welfare coordinated events, issued guidelines, and ensured that state health departments were in compliance with or in consonance with the guidelines issued by the ministry. Private practitioners, private hospitals, and nongovernmental organization, energized activities along with the District Disaster Management Authorities or District Health Departments. Community leaders were also involved by dispelling rumors. At the same time, community leaders educated people to wash their hands before eating and cover their faces while sneezing or

---

tial service providers was initiated as a priority. To develop the Business Continuity Plan for Non-Health Sectors, NDMA issued guidelines on influenza H1N1.

[29]Due to the effective response in India, there was minimal impact of the 2009 H1N1 pandemic. In India, the Ministry of Health and Family Welfare (MoH&FW) coordinated the entire response across the country and helped state governments in critical areas. State governments managed the pandemic following guidelines issued by the MoH&FW. The private health sector through Public Private Partnerships, non-governmental organizations, The Red Cross, and The Indian Medical Association worked with district authorities. Community leaders were involved for awareness to curb rumors and to coordinate with government agencies. Essential services in non-health sectors were maintained by the Department of Food, Water Supply, Transportation and Telecommunications, etc. Individuals and families were provided with personal hygiene information, such as the importance of washing hands, covering one's mouth and nose when sneezing and coughing, and home quarantine.

coughing to prevent infections. They also ensured that non-health services were also maintained. NDMA coordinated and monitored all events throughout the country and ensured that contingency plans were made available in all the states. At the same time, NDMA was also monitoring the status of H1N1 throughout the world. In addition to the role of the government, pandemic response planning takes into account the need to coordinate with industry, civil society, and local communities. This holistic approach is needed to provide medical interventions, such as distribution of drugs and vaccines; nonmedical interventions, such as quarantine; social interventions, such as communications; and essential basic services, such as security, food, water, and power.

Bansal stated that under current circumstances there is a threat of biological terrorism against innocent people around the world. To fight terrorist threats, comprehensive, preventive measures need to be planned and countries need to be fully prepared to handle an epidemic arising from such an eventuality. Bioterrorism will most likely be multinational, leading to a pandemic; therefore international cooperation will be of immense value for biodefense. Global disease surveillance, health intelligence, incorporation of WHO guidelines, quarantine at airports, utilization of global outbreak databases, and alert and response networks are the major components of pandemic preparedness plans and must be undertaken well in advance of an incident. In conclusion, cooperation on the exchange of information and experience, and the sharing of global best practices, modern technology, equipment, and skills among nations are the need of the hour in responding to a bioattack of international concern.

DISCUSSION

The discussion began with a question regarding how to deal with a combination of open information and rogue labs. Franz stated that because this is difficult, scientists must work together. Further, it is more likely that there would be a rogue individual than there would be a rogue lab because labs are hard to isolate internationally.

Norman Augustine then asked a question of Bansal about whether medical workers who are likely to come in contact with diseases during an epidemic should be required to be vaccinated in advance against known threats, for example, smallpox. Or is the risk of vaccination on such a large scale greater than the benefit to be gained? Bansal replied that in India officials try to vaccinate some groups of first responders, for example, the National Disaster Response Force (NDRF) and the Delhi police, but one has to weigh the benefits against the risks. There are considerably high risks associated with the anthrax vaccine, but fewer risks are associated with the polio vaccine, which is also less likely to be a bioterror agent. Clearly, one has to weigh the costs and benefits, even for the vaccinations against H1N1.

A workshop participant asked Franz about the screening of scientists and ethical issues: For scientists working in critical labs, what concrete steps should

be taken to avoid an incident such as the anthrax attacks, where a scientist may do something mischievous?

Franz began first by stating that he cannot promise that any actions will work. He could not guarantee that there would not be an insider threat in his laboratory. However, one can reduce the likelihood through the leadership and cultural approaches he discussed. If the director of a laboratory and everyone in that lab, no matter their rank, knows they can walk in and talk to the director if they want to, that culture of openness will likely help. The director may reinforce that there may be situations in which he or she needs to use the chain of command, but there might be times when someone is so troubled that the person does not want to talk to someone in that chain. These sound like fairly soft and squishy solutions, and they are very hard to scale. If we have 10 army labs in the United States and we wanted to do this in every lab, it would probably be impossible. But openness, transparency, focus on quality, support, and the people at the bench are more important. Seemingly small actions by the director, like asking his assistant to block out time every week for him to just go walk around the labs and talk to people, are critical. Scientists love to share their results. By listening and responding, Franz believes a healthier culture is built, and there is a greater chance of finding an outlier and dealing with that outlier. Franz added that when he was at the lab, background checks were not performed, but after the anthrax letters, FBI background checks have been conducted on everyone. The participant followed up by asking if there are objective methods that can be developed for background checks. Franz replied that Bruce Ivins had a number of background checks, including by the FBI. We do not know for certain if he was the anthrax mailer, and there is no definitive evidence that he was. However, the circumstantial evidence is overwhelming that he committed those actions.

Bansal continued the discussion by noting that labs are not the only places of concern. In any place that needs to be protected, one has to develop methodology that applies universally. First, a person responsible for a particular task has to be held accountable. Within any organization, there are different levels of security and different types of people. One approach is the two-person rule, as is used in the BSL-4 lab at the National Institute of Virology in Pune. In addition to subjective approaches, objective measures are also needed, such as background checks. Those who work in sensitive positions in India have background checks and are monitored.

Based on his experiences as director of the Defense Research and Development Establishment (DRDE) in Gwalia, which has expertise in handling chemical and biological terrorism **K. Sekhar** relayed what happened in India after the anthrax attacks in the United States. There was a barrage of letters that contained white powder addressed to various members of parliament. At one point, they received nearly five hundred to a thousand envelopes containing white powder. It took quite a while to go through and analyze all the powder. Sekhar assured members of parliament that the substance was nothing but chalk powder; however, the fear created was enormous. After those events, India began a major program to train forensic experts. Over the 4 to 5 years of his ten-

ure, every forensic laboratory in the country received training on emergencies related to CBRN.

The same participant asked Bansal about the reliability of biosensors and whether there is a regular system of standardizing the precision and accuracy of biosensors to avoid false positives and false negatives. Bansal replied that the accuracy of biosensors is dependent on knowing the baseline of the biological agent naturally occurring in the background.

Another question pertained to the availability of emergency equipment and medical supplies such as masks and antibiotics, for India's population of 1.2 billion people. Bansal replied that India has a high degree of preparedness, as the success story with H1N1 indicates. India does stockpile drugs for a certain number of people, and there are the commonly used antibiotics and detection equipment that could be sent from one part of the country to another. India is fully prepared, he said. There is also a stockpile of masks, but people must be educated on the need to use them. In terms of disseminating information, NDMA has a community-based disaster management plan that educates communities. For example, during the events in Fukushima, Japan, people in India received messages on their telephones stating that there would be acid rain in India, so they should not come out of the house. Bansal appeared on television and told people that Japan is about 6,000 kilometers from India and the direction of the wind is northeast; therefore, it was not blowing in the direction of India. There was no question that anything was coming to India by way of rain, wind, or sea. One has to develop a strategy to curb rumors and panic.

A participant asked about botulinum toxin because, he said, it is the only toxin that might be used in a terrorist attack. Russia is reported to have a large amount of botulinum toxin, and now it is on the open market for medical prophylaxis as well as for cosmetic uses.

Franz replied that botulinum is an interesting toxin. It is the most toxic substance known. It is a large, 50 kilodalton protein and it is not very stable, especially when it is purified. In former biological weapons programs, both the United States and the Russian Federation conducted work on it, but stopped. The Iraqis also tried to work with it. It is best not to stabilize it. It is denatured when it is very pure. The material that is used medically is very pure, because an immune response to some of the chaperone proteins occurs if it is not purified. Therefore, in order to have toxicity, it has to be injected or taken orally. It is not a very good aerosol weapon because it is not very stable and because it appears that macrophages in the airways destroy it. Also, there is a significant latent period. Franz did studies in nonhuman primates on inhalation methods, and then trying to treat them with antibodies as soon as they started showing clinical symptoms, and that was usually too late. The very first visible clinical signs are some changes in vision, and even if treatment starts early, it is probably too late. Then a ventilator is needed to keep the subject alive, and depending on the serotype, this could be for up to 30 days sometimes. A concern about botulinum would be contamination of something like milk.

A participant asked about the low mortality rates in the United States due to H1N1, because, unfortunately, the mortality rate was higher in India. What, he asked, was the strategy in the United States for the distribution and use of Tamiflu? With regard to Tamiflu and H1N1 in the United States, there was a great deal of monitoring to determine whether there was resistance developing. However, the United States focused on vaccines as the first line of resistance and Tamiflu was used only in specific cases. A participant noted that studies were conducted in Japan over the last 10 years on the medical prophylaxis of Tamiflu and very insignificant levels of resistance were found. Since resistance does not seem to be a problem, Tamiflu could be more widely distributed to help control the spread of the infection.

A final question was asked about mass monitoring of the public, for example, of people getting off airplanes and infrared scans being taken of their foreheads to see if they have a fever or not. Civil liberties seem to get in the way of this type of monitoring. Is that a good thing to do? And if it is, how do we deal with civil liberties issues? Bansal replied that monitoring is not for fever symptoms because there are so many causes of fever, and only a medical exam can determine the cause. As a doctor, he understands that careful observation is critical, and one cannot jump to a particular treatment until the particular cause is known so that the treatment will not change the course of the disease and affect the ability to determine the actual cause.

TECHNICAL ASPECTS OF NUCLEAR SECURITY

V. S. Ramamurthy introduced the presentation of the joint NAS-National Institute for Advanced Studies (NIAS) report entitled, *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security*.[30] He noted that one of the primary goals of the workshop was to jointly develop proposals for cooperation on nuclear materials security among experts from India and the United States. This challenge is complex and requires a multidisciplinary approach. He expressed his delight at the publication of the joint report that captures the 2013 workshop and highlights what we can do together to identify solutions.

Ravi Grover thanked Ramamurthy for the opportunity to speak at the formal Indian launch of the joint report. He reaffirmed that security of materials, facilities, export controls, and technologies associated with nuclear materials is taken very seriously in India, as is the development of proliferation-resistant technology. Using science and technology, one can reduce the magnitude of the problem of nuclear materials security. He noted that the nuclear security summits have raised the level of concern about nuclear materials security, and dis-

[30]National Research Council. *India-United States Cooperation on Global Security. Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security*. Washington, D.C.: The National Academies Press, 2013.

cussions have taken place on all aspects of nuclear security, including the global security architecture, the role of the International Atomic Energy Agency, the security of nuclear materials and radioactive sources, the nexus between nuclear security and nuclear safety, the security of transportation, combatting nuclear trafficking, nuclear forensics, and, most importantly, nuclear security culture, especially in industry. India has participated in each of these summits. As a part of the summit process, communiques and work plans have been issued, indicating the commitment of participants to nuclear security. Many countries have come together to offer gift baskets to do more than what is included in the communiques.

Another effort is the Nuclear Threat Initiative Nuclear Materials Security Index,[31] and one gets the sense that people are looking at the issue of nuclear security differently by focusing on disarmament and the elimination of weapon-grade materials. The way that this is viewed by some, however, may be a confirmation bias. Nuclear security needs to be examined without a confirmation bias in that there needs to be independent assessments of security that do not simply endorse the status quo without actually testing the system rigorously. One has to look at synergy between nuclear security and science and technology to reduce the overall problem. Nuclear materials are used in the generation of energy, which is especially important in India.

L. V. Krishnan stated that the 2012 workshop provided a wealth of information, just as this workshop is doing, but was more specifically focused on nuclear facilities and issues of nuclear materials security. It was an excellent opportunity for professionals to interact and share their perspectives, experiences, and programs. Speakers came from the United States with diverse experience in a range of aspects of nuclear materials security, including handling, which is large scale in the United States, and which requires advanced techniques of nuclear materials accounting, for example. Though production of materials in the United States has stopped, there is still a need for safety and security. India has developed in-house expertise, and they have made use of limited materials. Based on Indian power needs, experts have continued to work on developing proliferation resistant reactors, and reprocessing techniques are also being developed.

Krishnan also noted that there are links among safety, security, and safeguards, and there is a need for balance between the conflicting desires for greater transparency for the sake of safety, and the requirement for confidentiality for security purposes. Materials, control, and accounting require the right type of nuclear instrumentation for detection, and the quantification of nuclear materials. Non-destructive assay is a technique of mass spectrometry that provides near real-time information on nuclear materials and utilizes nuclear detectors and instrumentation. However, some materials are always left over in the plant, and this discrep-

[31]Nuclear Threat Initiative. Nuclear Materials Security Index. Available at: http://nti index.org/; accessed September 21, 2014.

ancy in material inventory is called materials unaccounted for. New real-time accounting techniques can help in material balance areas. Physical security is developed specifically for every facility, even for reactors of the same design. This is called the design-basis threat (DBT). The DBT, which is designed by scientists, law enforcement personnel, and security professionals, and includes training and requires training, was discussed as essential to security. In India, the Global Center for Nuclear Energy Partnership (GCNEP) has a school of nuclear security studies, which has been set up to train people.[32] The threats being considered are external forces, sabotage, and terrorism from the sea.

Krishnan also highlighted nuclear forensics, which involves analysis after capture, age, and isotopic composition. It is an imprecise science. Databases are critical and a national database is the first step in being able to have a library of forensic samples. In the United States, there are 300 samples in the national databases.

With regard to cybersecurity, software needs to be tested often, because the use of commercial systems has its risks and unknown vulnerabilities. The Security Network Access systems used at Indian facilities have different zones with firewalls. However, unless the digital systems are appropriately secured, increasing the level of connectivity of many critical facilities may actually introduce more vulnerabilities and increase the risks of cyberattacks.

In conclusion, there were numerous suggestions about cooperation on safeguards, safety and security. There is common ground on the importance of detection and of tracking materials to maximize safety and security. Spent fuel may be used as a means of exploring these issues together. Not all lessons, however, can be directly transferred from one place to another, so we need to take context into account.

Raymond Jeanloz stated that we have a great deal of agreement on the Indian and U.S. sides. The focus of the workshop was on civil nuclear materials and technical aspects because we come from the technical communities in our countries. The background for the workshop was the nuclear security summit of 2010 and one of the outcomes of that summit was a commitment by the Indian government to establish the GCNEP.[33]

---

[32]The school's mission is "To impart training to security agencies on application of physical protection system and response procedure, to enhance physical security of nuclear facilities by developing and deploying most modern technological tools including information security and to provide facilities for test and evaluation of sensors and systems used for physical security." Government of India, Department of Atomic Energy, Global Centre for Nuclear Energy Partnership, School of Nuclear Security Studies. Available at: http://www.gcnep.gov.in/schools/snss.html; accessed September 21, 2014.

[33]Cann, M. *2010 Nuclear Security Summit National Commitment Implementation: Steps in the Fight Against Nuclear Terrorism*. Paul H. Nitze School of Advanced International Studies (SAIS), Johns Hopkins University. U.S.-Korea Institute at SAIS, 2012. Available at: http://uskoreainstitute.org/wp-content/uploads/2012/03/USKI_NSS2012_Cann.pdf: accessed September 21, 2014.

Civilian nuclear materials are found in many countries, and the tracking of materials is less perfect than one would like, as we need to balance nuclear energy and nuclear capacity with nuclear security. Jeanloz emphasized the systems approach to nuclear security, and noted that the report raised the importance of comparing notes among Indian and U.S. experts to this end.

Communication with the public is also crucial, and the point was made in the report that the technical community needs to think about this communication in advance because the public and policy makers need to be convinced that the solutions are reliable and can be trusted.

Focus on future collaboration leads to discussion of technologies and larger-scale systems integration. Built-in validation will help to mitigate problems of human reliability so that people stay alert and are notified that they are performing well. This means integrating hardware and software with the psychology of individuals and culture; this is another imperfect area where we can work together.

Jeanloz noted that there are strong capabilities in both the United States and India, but the interpretation of results is still somewhat an art form. It is not enough to have a complex understanding of a sample since decision makers need to have attribution for actionable intelligence. There may be pressure for a rapid turnaround of information. There are many areas for cooperation in this regard. For example, we could begin by analyzing facilities in the field and start building databases, because we need to have something to compare against. There is also a need for more specific understanding of processing materials, age dating, and chronological analysis. An effective program will require international cooperation. There are technical ends and political ends: databases need to be compiled and different countries or groups have databases that need to be made more available via technology while still protecting the confidentiality of the samples. It is not necessary to share the details when querying a database.

Insider threats are also a challenge because we do not have enough ideas about how to identify an insider and to act on this knowledge. There are technological solutions that need to be developed beyond Personnel Reliability Programs (PRP). Examples of possible technical solutions include delay mechanisms to control access to critical areas, observation cameras, and material balance techniques to monitor movement and use of sensitive materials.

Jeanloz concluded by saying that a key to this report was highlighting the potential for cooperation among experts from Indian and U.S. national labs, academic labs, and industry. It was very clear that the technical communities continue to want to work together, and we can benefit from working together.

DISCUSSION

A participant asked if security classification is based on legal and predetermined criteria. **Michael O'Brien** replied that if we analyze security, there are systems that are classified, and there are classification guides that are descrip-

tions of a detailed protection system that someone may exploit. Every country has its own security systems and no matter what they want to share, they cannot.

Micah Lowenthal also noted that one can discuss safety systems without giving away too much because one can talk about reliability, and this can help provide confidence to people. With regard to the threat, there is very little that is shared publicly and DBT is not shared. There have been proposals for international databases on forensics, but the United States has been promoting the idea that each country should have its own database so that if there is a question, we can be confident that another country could answer that question for its own purposes.

A participant asked about cyberthreats and the inadequacy of psychological threat analysis. If one takes a large number of cases, there will be people who are doing bad things, including killing people. Close observation of people alone does not always reveal these problems. Are there other means of psychological testing that can provide confidence in the psychological fitness of the employees in sensitive facilities? Would an approach such as "know your employee" help increase this confidence?

Jeanloz replied that PRP is the type of detailed program that is used as a means of evaluating threats, and some are common-sense practices, such as routine testing for drugs and alcohol use, just like for pilots. Yes, there are a number of these tests that are used. He did not want to diminish these practices, but perhaps there are some other technological solutions, such as the two-person rule or engineering solutions to make it difficult to subvert the system. We could benefit from another round of joint discussions on this because there may be technologies that can help build a difficulty for misusing the system.

O'Brien noted that at the 2012 workshop, an overview of a 2-week training session was given. The training deals with insider threats, identifying anomalies, engineering out potential vulnerabilities, recognizing insider threats, and addressing operational aspects of facilities. This is an area ripe for cooperation.

Mukkamala noted that after an incident, such as a school shooting, people can work backward to identify threats; companies do this as well. One can be persuaded to provide this information, and industries sometimes do this.

Grover made a final comment. There is a lot of tension at the present time because, on one hand, civil society demands transparency, and on the other side, there are technologists and bureaucrats who feel the need to protect sensitive technologies. How do we balance these two perspectives?

Jeanloz agreed that this is a challenge and added that the problem is even greater because there is a tension between privacy and the tracking of technology to depersonalize the discussion; we allow ourselves to be tracked by companies. Transparency vs. sensitive information and tracking of information is what social media is doing. For our democracies, there is a debate on the nature of privacy. Is privacy gone? We should not jump to this conclusion. Augustine added that in his view, privacy is gone. The CEO of one of the better known web-based social sites said that one can build tiny cameras and people leave

cameras around the home and post videos on the web that they cannot get back. The CEO said simply, "Get used to it."

FROM SUGGESTIONS TO COOPERATION

Stephen Cohen noted that his overall concern was for the output of the workshop to not disappear into space. Converting technology insights into useable policy recommendations is the most difficult task of all. So how can we convert ideas and suggestions into policy that will be implemented? This involves interface with the policy community, the media, and politicians.

Politicians are busy people. They need material that they can understand and that allows them to prioritize the way in which they spend money and the way in which they allocate time. That is the major task. What we have done at this workshop thus far is a superb, world-class discussion of how technology can influence the prevention of terrorism, and amelioration of terrorism, but how does that translate into words that a politician can understand? How do you do things that get people to do the right thing without forcing or coercing them? One of the key points Cohen learned is that the responders to a disaster or a terror event must keep ahead of the media or keep current with the media because the media have a life of their own, especially social media.

Cohen offered a practical way forward: make a comprehensive list of potential areas for cooperation. That forces people to think about priorities. What is the most important issue? What is the least important issue? How does one balance out chemical threats, biological threats, nuclear threats, cyber threats? Politicians must demonstrate why things that do not appear to be a threat now might be a threat in the future, and why they are worth attention and perhaps money and time, which, of course, is the scarcest resource of all in governments.

In particular, what about the whistle-blower effect both in governmental organizations and in private organizations. How does one get companies or perhaps government units to behave responsibly in terms of developing protected devices when it is not profitable to do so?

Cohen has learned that an efficient system, one that is geared to protect against terrorism, is actually more profitable in some ways as well. There is less waste; this is the case with the use of baggage tags, and tagging of containers. The system actually works better when one prepares for security in many ways. The additional cost of security may actually be regained in terms of efficiency of plant operation and so forth.

A point that A. K. Sinha made is that preparation for disasters may have spin-off effects for other threats, including terrorism and vice-versa. Perhaps in a future meeting, we can explore the relationship between disaster preparedness and terrorism preparedness. If money is spent on disaster management, for example on a national disaster management center, competence in terms of terrorism management is improved.

Cohen wrote a book in 1978 about the Andhra Cyclone and clearly, India has improved preparedness and response to cyclones to a level better than Amer-

icans, as seen during Hurricane Katrina. Sinha thinks the government had looked at the Orissa case here, also. When government reviews their own performance and it improves, they inspire confidence in their people and their populations. This applies to terror attacks as well as natural disaster events.

Cohen also proposed a new meeting on the question of implementation. When he first came to India 50 years ago, almost to the month, he attended several Indian National Congress Party meetings. The one Hindi phrase that was burned into him quickly: "We must implement. We must implement." He has heard this phrase often ever since. It was astonishing.

V. J. Sundaram stated that the systems approach has been stressed with the need for quality reviews, testing, maintenance, training, retraining, and finally accrediting the whole system. He agreed that implementation is key. Whether it is for tackling national industrial disasters or emergencies or for terrorism response, which will reduce vulnerability, he thinks that using systems engineering designed for Six Sigma certification makes systems more reliable and robust. It takes time, however. As an engineer, he was glad that the question of whether India needs a better quarantine system for agricultural and food was emphasized. The same thing with health; proactive measures helped India to contain H1N1.

5

Emergency Management and Response: All-Hazards Approach

U.S. AND INDIAN EXPERIENCES WITH EMERGENCY MANAGEMENT AND RESPONSE

American Experience during Hurricane Katrina and Superstorm Sandy

Karl Kim began his presentation by describing the National Disaster Preparedness Training Center (NDPTC), which is a Federal Emergency Management Agency (FEMA) center and part of the National Domestic Preparedness Consortium, which he directs. The consortium was created after the Oklahoma City bombing and was greatly expanded after the September 11, 2001 (9/11), terrorist attacks.[1] After Hurricane Katrina, the University of Hawaii was added as one of the consortium's members. The NDPTC at the University of Hawaii develops and delivers training courses on natural hazards and various tools related to disaster risk reduction, response, and recovery. The center also works on threat and hazard identification and risk assessment tools to integrate both a national perspective and state and local perspectives. Geographically, the center focuses primarily on the Asia-Pacific region, one of the most dynamic in the world, in which there are many different regional entities and groups organized for security, trade, environmental issues and so forth.

Security of the American homeland arguably started in the 1920s, focusing on civil defense and in the 1970s FEMA was created, and there was an increased awareness of natural hazards. Terrorism events—the Oklahoma City bombing, and the attacks of 9/11—broadened the scope of what the organizations that became the Department of Homeland Security covered. The responsi-

[1]The U.S. Federal Emergency Management Agency. National Domestic Preparedness Consortium. "Preparing the Nation through Training." April 29, 2014. Available at: https://www.ndpc.us/pdf/2014%20NTE%20PRESENTATION%20TEMPLATE_CS3%20NPDC%20Final.pdf; accessed September 21, 2014. See also, "Letter from the Chairman." *NDPC News*, Vol. 3, Issue 3, Summer 2008. Available at: https://www.ndpc.us/pdf/NDPCNews3.3.pdf; accessed September 21, 2014.

bilities are very broad and that scope tends to be event-driven; one of the largest recent events in the United States was Hurricane Katrina, which caused FEMA to further evolve. The current framework for emergency support functions in the United States is laid out in the Presidential Policy Directive 8, the Stafford Act, and the National Preparedness Goal, and recently the emergency support functions have widened to include recovery support functions.[2]

The Asia-Pacific region also has the greatest rates of urbanization in the world, and some of the fastest rates of change are occurring in countries like China and India. Kim believes that cities should be units of analysis for studies related to emergency response because they are critical leverage points, and because cities allow one to maintain perspective better than if the unit of analysis was a large geographic area such as a country or the world. Cities are also a source of solutions, not just sources of challenges.

Kim then turned to a comparison of two significant events in detail: Hurricane Katrina and Superstorm Sandy. As Hurricane Katrina passed over the Bahamas, it intensified and first made landfall in Florida on August 25, 2005, and then made landfall in Louisiana on August 29, and it actually weakened when it hit Louisiana. Superstorm Sandy was different. It also developed in the Caribbean, and then its peak intensity occurred prior to landfall in Cuba when it became a hybrid storm. It made landfall in the United States on October 29, 2012. Hurricane Katrina was a very compact and intense but big storm, whereas Superstorm Sandy was much larger and in many ways diffuse, causing a variety of effects. It caused wind in some areas, but it also brought snow. Hurricane Katrina had more significant winds, whereas Superstorm Sandy had everything from blizzards in the Appalachian Mountains to flooding in Manhattan. With both Hurricane Katrina and Superstorm Sandy, there was an increase in the seawater level, causing a storm surge. More than 1,800 people were killed as a result of Hurricane Katrina, and damages totaled approximately $108 billion, which made it the costliest hurricane in U.S. history.[3] As a result of Superstorm Sandy, 147 people died and damages totaled approximately $50 billion, but there were also

[2]U.S. Department of Homeland Security. National Preparedness Goal. 1st ed., September 2011. Available at: http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national_preparedness_goal_2011.pdf; accessed September 21, 2014. And, U.S. Department of Health and Human Services. Public Health Emergency, Emergency Support Functions. "Emergency Support Functions is the grouping of governmental and certain private sector capabilities into an organizational structure to provide support, resources, program implementation, and services that are most likely needed to save lives, protect property and the environment, restore essential services and critical infrastructure, and help victims and communities return to normal following domestic incidents." Available at: http://www.phe.gov/preparedness/support/esf8/pages/default.aspx; accessed September 21, 2014.

[3]CNN Library. Hurricane Katrina Statistics Fast Facts. Available at: http://www.cnn.com/2013/08/23/us/hurricane-katrina-statistics-fast-facts/; accessed September 21, 2014.

significant effects on peoples' lives: an estimated 8.5 million people were without power, 650,000 homes were destroyed, and so forth.[4]

Kim was part of a FEMA reconnaissance team deployed immediately after Superstorm Sandy. The storm significantly affected two types of areas: urban areas and coastal areas. In urban areas like New York City, Lower Manhattan was flooded, basements were flooded, power systems were knocked out, and subway tunnels were flooded. On the coastal areas, the significant storm surge and flooding destroyed many buildings and structures. Disproportionately, elderly, people with disabilities, and poor people were negatively affected in this storm. An evacuation order should have been given in Kim's view, due to how quickly the water level rose and the threat of casualties in the New York City area. There was an assumption that Superstorm Sandy was going to behave a lot like Hurricane Irene, but it did not.[5]

Rae Zimmerman at New York University, together with the American Institute of Architects in New York, is mapping the locations of a variety of types of urban infrastructure, such as electrical power plants, wastewater systems, and transportation systems located below 10 feet or in coastal areas prone to flooding.[6] A plan was proposed by Jeroen Aerts of the Free University of Amsterdam to build a floodgate system to protect Manhattan for between $11 billion and $23 billion.[7] The question is, where will that water go if it is prevented from going into Manhattan?

Kim then compared Superstorm Sandy to previous hurricanes in terms of the number of homes destroyed, the damage in dollars, the number of people evacuated, and the number of fatalities. When compared to Hurricane Camille (category 5, one of the biggest storms),[8] and to Hurricane Ivan, a category 3

---

[4]Blake, E., et al. "Tropical Cyclone Report, Hurricane Sandy." National Hurricane Center, National Oceanic and Atmospheric Administration, February 12, 2013. Available at: http://www.nhc.noaa.gov/data/tcr/AL182012_Sandy.pdf; accessed September 22, 2014.

[5]Rice, L. "An Analysis of Public Perception and Response to Hurricane Sandy" (master's thesis, Univ. of South Florida, 2014). Available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=6310&context=etd; accessed September 22, 2014.

[6]Zimmerman, R., and Faris, C. "Infrastructure Impacts and Adaptation Challenges." In *New York City Panel on Climate Change 2010 Report*, pp. 63–85. Available at: http://macaulay.cuny.edu/eportfolios/bird2012/files/2012/07/Infrastructure-Impacts-Adaptation-Challenges.pdf; accessed September 22, 2014. See also: NYC Planning. *Coastal Climate Resilience, Designing for Flood Risk*. Department of City Planning City of New York, 2013. Available at: http://www.sustainablenyct.org/news/NYCDCP_DESIGNING%20FOR%20FLOOD%20RISK_DRAFT-LOW.pdf; accessed September 22, 2014.

[7]Aerts, J., et al. "Cost Estimates for Flood Resilience and Protection Strategies in New York City." *Annals of the New York Academy of Sciences*. New York: New York Academy of Sciences, 2013. doi: 10.1111/nyas.12200. Available at: http://www.ivm.vu.nl/en/Images/nyas12200_tcm53-364896.pdf; accessed September 22, 2014.

[8]Associated Press. "Hurricane Camille's Peak Winds at Coast Downgraded." *Washington Times*, April 9, 2014. Available at: http://www.washingtontimes.com/news/2014/apr/9/hurricane-camilles-peak-winds-at-coast-downgraded/; accessed October 20, 2014.

storm,[9] many more people evacuated during Superstorm Sandy. Hurricane Katrina was not particularly damaging along the coastal area of Mississippi, but with the effects of flooding and the breaking of the levy in New Orleans, many more people were killed. Kim also compared Hurricane Katrina to a high-end typhoon in the Philippines, which caused 6,200 deaths.[10] The damages were much lower in terms of dollar value, only about $15 billion, but many more people were displaced and adversely affected in the Philippines.[11]

Kim is working on a federal highway project that involves assessing effects on transportation by examining different risks, hazards, and threats, then focusing on the inventory itself and what needs to be protected. The same kind of logic that applies to security assessments applies to this analysis as well. In order to conduct long-term planning for prevention and response, Kim and his colleagues are modeling various effects of sea-level rise, hurricanes, storm surge, tsunamis, and river flooding on cities to determine the impact of an overall rise of 1-meter by 2100, which most experts agree will occur. They are interested not only in average sea levels, but also in the increase during extreme events; therefore they have been examining the effects of recent flooding that is not related to storm surge or surf. Flooding occurred at Waikiki Beach in recent years and in the winter of 2013, which caused significant damage. The water drainage system is backed up with sea-water and the resulting effect is being seen.

One of Kim's colleagues at the University of Hawaii has shown that as the sea level rises, the freshwater level also rises and produces increased flooding in urban areas. Therefore, much more of the urban area will be flooded due to the rise of groundwater levels, as well as the intrusion of seawater. As a result, part of the mapping involves trying to understand the combined effects of sea level rise and tsunamis, and sea level rise and other hazards. Further, Kim and his colleagues are using asymmetric mapping techniques to identify the exposed population by flooding depths and then applying that information to an assessment framework to attempt to predict possible events, focusing specifically on criticality. Which place will receive the worst flooding? Which place will be most negatively affected? Where do seniors live? Where are the most socioeconomically vulnerable people located? Where are critical infrastructure systems located? It is very difficult to predict the locations, but we know the most critical

[9]CBS Miami. "Florida Marks the 10th Anniversary of Hurricane Ivan." September 16, 2014. Available at: http://miami.cbslocal.com/2014/09/16/florida-marks-the-10th-anniversary-of-hurricane-ivan/; accessed October 20, 2014.

[10]CNN Staff. "Typhoon Haiyan Death Toll tops 6,000 in the Philippines." December 13, 2013. Available at: http://www.cnn.com/2013/12/13/world/asia/philippines-typhoon-haiyan/; accessed October 20, 2014.

[11]"Of the 15 million people in the Philippines affected by Typhoon Haiyan, around 4 million have been displaced from their homes, including more than 94,000 living in 385 evacuation centres." United Nations Children's Fund. Available at: http://www.unicef.org/infobycountry/philippines_71516.html; accessed September 22, 2014.

systems in terms of demand, so combined risk scores are developed to understand how to apply the framework.

Kim focuses specifically on trying to understand travel behavior. For example, based on travel demand surveys, Kim can determine that all of a person's trips in a given day are in the flood zone, and then he maps trip origins and destinations by flooding depths and models travel demand during hazardous events. It is very difficult to simulate behavior during an event itself; therefore, what he has been trying to do is determine how to integrate global forecast information and other data into the framework.

Another application of Kim's research is to integrate public alert systems including not just radio and television, but also smart phones and other devices to assist in evacuation modeling. All of the sirens and warning detection systems are designed primarily for tornadoes and tsunamis, less for flooding in vulnerable communities. One of the problems he found was that many of the evacuation centers or shelters are located in the flood zone. Which responses, including detection, warning, and evacuation are most effective? What is the range of strategies that can be used to improve responses?

Kim and his colleagues have been developing a tsunami preparedness model that focuses on nuclear power plants and associated issues. Kim noted that in the Japanese case, multiple precautions were taken, and almost every one of them failed. Kim's future work involves refining this information and focusing on critical lengths or segments of urban environments because obviously with sea level rise, more areas will be flooded. He and his colleagues are moving away from the paradigm of "fail-safe" to "safe-to–fail" approaches, rethinking zoning or no-build zones.

In conclusion, Kim underscored that urban technology is getting faster and smaller, and has increased connectivity. The notion is that humans are now the ultimate sensors through personal electronic devices such as smart phones, from earthquake detection to information about storms. These technical changes also change notions of security, and today, almost everyone has a camera on a smart phone. Even though there is some resistance to security systems, video cameras are prevalent. This is actually an old concept, called the panopticon, which was a system of construction designed by Jeremy Bentham for surveillance in prisons, schools, and factories. Bentham's idea was that one could, by design, create an environment where the people are knowingly always observed, resulting in complete security and no privacy.[12]

Indian Experience during the 2013 Himalayan Tsunami

Shri Vinay Kajla prefaced his remarks by stating that he is a member of the Central Industrial Security Force (CISF), which handles security for India's

[12]University College London. "The Panopticon." Available at: http://www.ucl.ac.uk/Bentham-Project/who/panopticon; accessed October 20, 2014.

airports, seaports and all Indian nuclear power installations. CISF was one of the organizations that responded to the Bhuj earthquake in 2001 by addressing response needs at the airport. Kajla led a small team of approximately 320 people from his fire department in that response. Their first observation was that there was a large number of aircraft with a great deal of equipment but there was no one to unload it. Initially, there was reluctance by the air force to accept help from Kajla's group, but eventually his company of 320 men unloaded nearly 120 aircraft. The International Red Cross wanted to put up a 400-bed hospital and with the help of Kajla's team they were able to get it going. The CISF team also helped a 50-bed Israeli hospital become operational. Rescue teams arrived from several countries, including Denmark, Switzerland, and the United States, bringing specialized equipment that India did not have.

The severe floods of June 2013 affected five districts[13] and were caused by extensive rainfall that fell in just 48 hours (see Figure 5-1). Normal annual rainfall is approximately 26 millimeters, whereas in this period alone there was 400 millimeters of rainfall. The heavy rainfall triggered a large number of landslides and even the movement of a glacier. Kajla noted that in the most affected town, Kedarnath, nearly 5,000 people died, including numerous tourists. In addition to the loss of human life, many mules that carried tourists to temples also perished. Large construction projects had been built all along the riverbed itself, which also contributed to the vulnerability of the riverbanks to landslides. The local temple was located on a foundation of large, heavy stones, but was washed down the hill within 3 minutes, starting at 6:37 a.m. on June 16, 2013, leading to the total destruction of the towns below. A brand new building unfortunately no longer exists because it was constructed too close to the river bank. This is a clear example of the importance of zoning and adherence to zoning regulations.

Given the destruction of nearly all of the roads leading to the site, the only way to evacuate victims was via one of a few Mi-17 helicopters that can carry 25 people or perhaps 30 if the helicopter is carrying less fuel weight. This limited capacity meant that there was a large number of people waiting to be evacuated. Although relief flights rapidly responded with deliveries of food and other necessities, during the initial 3 days the response from the state governments proved to be insufficient to meet the needs. Furthermore, heavy rainfall continued, and prepositioning of fuel at the airstrip below was inadequate to allow flights to keep up with demand. When combined, these operational challenges limited the effectiveness of the relief response. The response effort proved dangerous not only to those who were attempting to evacuate, but also to the National Disaster Management Authority (NDMA) responders. In one case, an Mi-17 helicopter crashed, killing 20 people, of whom 9 were Kajla's colleagues from NDMA. Reflecting on the implementation of response efforts during this

[13]The five districts were: Bageshwar, Chamoli, Pitho-ragarh, Rudraprayag, and Uttakashi.

FIGURE 5-1 Heavy rains on June 16 and 17, 2013. The floods of June 2013 affected five districts in India; the town of Kedarnath was most affected with 5,000 deaths. SOURCE: Kajla, 2014.

disaster, Kajla concluded that there was fairly good coordination among the Indian Army, Central Paramilitary Forces, Indo-Tibetan Border Police (ITBP), and National Disaster Response Force (NDRF). ITBP responded with five battalions. NDRF took in 450 responders and evacuated a large number of people over specially constructed bridges, and using their helicopters.

Among the challenges India faces in preparing for and responding to such incidents and disasters is the equipment procurement process. As a result, good communication equipment such as mobile towers at the site of a disaster, and portable reverse osmosis drinking water systems unfortunately are not available to first responders.

The fifth meeting of NDMA, held in October 2013, strengthened their commitment to disaster preparedness by, for example, creating a network of available helipads in advance of an incident. They will try to earmark funds for better observational and forecasting capabilities, improvements in communication infrastructure, restoration of roads, and the building of multidisaster shelters. These are the key areas on which the government of India would like to focus in the next 2 to 3 years to improve preparedness in the high-altitude and hill states.

The government is also encouraging those responsible for private structures, such as religious sites, to prepare for disaster in advance as well. There are temples designed for a capacity of 1,000 people, but at times hold more than 7,000 people. This creates significant vulnerabilities; in one case, a stampede occurred and 250 people died while trying to evacuate a temple in the midst of a natural disaster.

Kajla concluded his remarks on the flash floods known as the Himalayan Tsunami by stating that it will be a long process, but India is making great strides in improving its preparedness and response capabilities.

Indian Experience during Cyclone Phailin

Kajla provided a brief presentation on improvements in disaster response as seen during the category 3 hurricane, Cyclone Phailin, that hit in October 2013.[14] This hurricane was the second most powerful hurricane in Indian history after the Super Cyclone of 1999.[15] Despite its force, only 25 casualties were reported as a result of Cyclone Phailin as compared to 9,894 casualties caused by the Super Cyclone.[16] This success in the number of lives saved is attributable to the fact that the advanced evacuation plan took a large number of people out of harm's way, and those who remained were protected in cyclone shelters. Kajla noted that this is where technology aided the government's preparedness efforts.

Accurate forecasting by the India Meteorological Department significantly contributed to responders' ability to concentrate preparedness efforts in the areas of greatest need. Teams were able to be positioned with necessary equipment well in advance of the storm. Specifically, the cyclone flood shelter was staffed with volunteers and had appropriate equipment. The Puja holiday of Dussehra is an important festival and fell just a day prior to Cyclone Phailin and so all activities were canceled by the Odisha State Disaster Management Authority, so as to take proactive steps. Free food stations were established and the evacuation process intensified and was concluded over 4 days. Section 34 of the Disaster Management Act empowers authorities to force people to evacuate wherever they are reluctant to move to safer locations.[17] In the final stages of preparedness, this statute was invoked by local officials helping to ensure the low fatality rate.

A large number of people responded and were well-coordinated with well-established communications. NDRF responded with 53 teams totaling 2,500 people, the largest-ever deployment in India to date. When the cyclone did hit, formal reports of damage in 17 districts indicated that there was a great deal of

[14]Cyclone Phailin made landfall near Gopalpur with a wind speed of 200 km/h.

[15]The 1999 Odisha Cyclone was the strongest tropical cyclone ever recorded in the North Indian Ocean. It developed over the Malay Peninsula and on October 28, it became a severe cyclone and hit India the next day as a 155 mph (250 km/h) cyclone.

[16]The cyclone dumped heavy, torrential rain over southeast India, causing record breaking flooding in the low-lying areas. The storm surge was 26 feet (8 meters). It struck the coast of Odisha, traveling up to 20 km inland. It caused the deaths of about 10,000 people, and heavy to extreme damage in its path of destruction.

[17]For the purpose of assisting, protecting, or providing relief to the community, the district authority may control and restrict the entry of any person into, his/her movement within, and departure from a vulnerable or affected area.

infrastructure damage in numerous villages. An estimated 90,000 houses were destroyed, but human casualties were low. Estimates of the cost of the damage were lower than in other disasters and are attributable in part to the circular design of some structures. Highway and energy infrastructure damage was largely repaired fairly quickly. Restoration of the water supply did take time but the Odisha state government addressed this issue quickly.

NDRF helped with removal of fallen trees immediately after the storm cleared. At 6:30 the next morning, before people woke up, NDRF was already cleaning up the highway so that infrastructure maintenance and repairs could proceed. NDRF also established medical camps at the site, and used disaster management equipment to open the doors as quickly as possible.

Looking forward, the World Bank and the Asian Development Bank conducted a study that was presented to the government of India, in which they suggested using underground cabling because India still has a lot of overhead cabling in coastal states. Following the "build back better" principle, India will transition to underground cabling for power and telecommunication systems.

DISCUSSION

Nancy Jo Nicholas framed the discussion period by underscoring the importance of thinking about the link between counterterrorism and natural disaster planning and resilience, and adaptability and sustainability. She believes that definitions of terrorism also include attempts to terrorize, frighten or scare people; however, increasing levels of preparedness counters these threats.

A workshop participant asked about the distinction between preparedness and response to terrorist incidents versus natural events. How does one make those distinctions and where is it useful to make those distinctions?

Kajla stated that NDMA was constituted to deal with natural hazards; however, terrorist incidents that lead to a similar kind of mass fatality situation will also require a coordinated response by all agencies, including the Ministries of Home Affairs, Defense, and other core ministries.[18] Any incident, whether man-made or naturally occurring, will require a humane approach to solve the problems of those affected. If agencies learn to cooperate and integrate, he said, most problems can be solved. Unfortunately, whatever lessons are learned along the way, they often take a long time to implement.

Kim replied that there are clearly differences in terms of the level of harm that can be caused by different types of hazards, storm surges, earthquakes, and terrorist attacks, and it is important to understand these differences. The concept

[18]Ministries and agencies include: Civil Aviation, Earth Sciences, Water Resources, Agriculture, Mines, Environment and Forests, Department of Atomic Energy, Heath and Family Welfare, Railways, Road Transportation and Highways, Urban Development, and the India Meteorological Department under Earth Sciences.

of criticality—the critical infrastructure systems that one cannot afford to lose for whatever reason—is essential.

Kim also pointed out that there is another type of hazard separate from a natural hazard or a man-made terrorist hazard: the hazard of poor planning or bad governance. Governance sets the context for how a risk assessment will be conducted, how the detection and warning systems will operate, and how communication with vulnerable populations will be addressed, which will ultimately determine the effectiveness of the response, especially in how quickly one can recover from these incidents.

A workshop participant noted that during and immediately after major disasters, space technology has a significant role to play, both in providing satellite imagery and in supporting communications for emergency terminals, satellite phones, and so on. In this context, one of the mechanisms for international collaboration that has been established over the years is the International Charter on Space and Major Disasters in which India and the United States are among 11 partner countries. The charter was activated for both Superstorm Sandy and Hurricane Katrina. Useful images were provided immediately after these events to assess the damage and also to inform appropriate response actions. Also, there was mention of the use of satellite imagery in the case of the Himalayan Tsunami. What is the effectiveness of the use of these images in tackling emergency situations?

Kajla replied that satellite images help in assessing what is happening, but from an operational point of view, real-time decision making has to happen on the ground. If there is a 13,000-foot mountain in front of you, images are good but you still need to walk up the mountain and take patients down from wherever they are stuck in the landslide. It also helps to assess aftereffects for reconstruction and rehabilitation, and long-term planning. In the immediate term, one has to be on the ground. Smaller unmanned aerial vehicles (UAVs) proved helpful in quickly assessing the situation, together with eyes on the ground. In one example, people were trapped between two landslides and even NDRF could not reach them and the army helicopter could not come close enough to the mountain. Finally, in the evening, a civilian helicopter managed to bring them out. For short-term issues, people are needed on the ground, but for long-term issues space images and satellite telephones are very important, because it will take days before normal communication returns.

Kim replied that there have been tremendous improvements in satellite imagery and access to this information. He pointed out that the imagery is very good for tracking and following a storm, but that is not the same as predicting the storm path. Even though we have become much better at predicting where the storms will make landfall, there was a controversy during Superstorm Sandy concerning predictions of the U.S. model and the European model. It is very easy to make predictions in the near term, but as one goes farther and farther out in time, predictions become more challenging. Kim's group at the University of Hawaii is one of the few programs to conduct minisatellite launches and they are

also attempting to put multispectral sensors on UAVs or smaller, shorter-range devices.

Another participant asked, what are the lessons learned for improving training for emergency responders after these disasters? Kajla answered that training for a wider group of people is a key issue because the emergency responders from NDRF will take time to reach the site of a disaster. Therefore, training of state-level forces is critical because the community response is the first line of defense. Unless communities are better prepared, we will continue to suffer fatalities. There are practical issues with regard to various facets of disaster response, which unfortunately still have to reach the grassroots level; hopefully, technology will be able to provide other alternatives. The only problem is that training courses are often so boring that people sleep through most of them. Disaster management by itself is a very difficult topic, and it is something that people do not want to consider. There is a common thought, "If I did without a seat belt for the last 30 years, why do I need to wear one now?"

Kim replied that for first responders, there are really only two different types of training required. One addresses incident command systems, such as the U.S. National Incident Management System. Standard operating procedures are essential, as is the link between training and equipment. At another level, there must be decision making in periods of uncertainty and decision making under stress. How does one create an environment where responders can make the appropriate decisions when they have limited information? How do they make very quick resource allocation decisions? That level of training, creating that kind of culture, is much more difficult than training on equipment. Kajla added that there are other characteristics that are required, such as experience in disaster management situations, in, for example, handling large crowds.

A workshop participant asked: How can mobile devices and similar technologies, which tend to be in the hands of wealthier members of the population and not as readily available to other populations, benefit the whole community? Kim said that there is such rapid evolution in digital technology that it is very difficult to anticipate and predict all of the innovations that may be forthcoming. Technology is evolving, and many vulnerable populations now have access to mobile devices, so this provides one way to reduce some of the disparities. Kim added that one of the truly remarkable things that FEMA has done is adopt a "whole community initiative." It is based on the recognition that the government cannot be all things to all people everywhere, and it is important to learn from communities and to empower them to take care of themselves. In the event of an emergency, chances are a resident or a community member would be the first on the scene. Also, there is a lot of indigenous knowledge, particularly about hazards and threats that exist in a community. In the race to adopt satellite communications and cell phone technologies, we should not abandon all of the wisdom and knowledge that exists with cultures that are particularly close to the natural environment and that have an understanding of the history and the place.

Further, what are the priorities if one has a limited amount of time but not a limited budget? What are some priorities for U.S.-Indian cooperation? Kajla

noted that it is difficult to identify priorities for international collaboration; however, a key area is training for communities. One can help people become aware of the simple steps that they can take. This has worked in the states of Assam and Bihar, which are prone to floods and where people wanted to save their communities. Therefore, on their own initiative, they made low-cost, low-floating aid devices that save their animals, resources, and lives and now have a very well-established system. Conversely, Kajla has been grappling with the problem of how to provide better water treatment systems during floods. The government does not own these systems but can procure them thereby enabling communities to recover more quickly from an event. This is an area that is open for cooperation.

A workshop participant shared experiences from the response to the 2004 Indian Ocean earthquake and tsunami. Nongovernmental organizations (NGOs) had a lot of money to rebuild infrastructure, but most built two-story buildings; Thai people in that particular region, however, were not keen to inhabit the second stories of the buildings. They used only one story and the second story often remained empty. Further, one of the NGOs, a heavily funded group, had a standard list of materials to be used, but the particular type of wood specified was not available, so funds were not made available for response to the tsunami.

Kajla replied that people in India had experienced the same challenges with international donations. In many Indian communities people do not wear jeans and tops although this is what was provided by international NGOs. Whatever we do in the spirit of help may not actually be helpful at the site of a disaster. It is important, therefore, to let donors know what they should do to help. Reconstruction is slow, and it is not a very publicity-driven process. Most people lose interest in a disaster site after a short while because the next disaster has already happened. However, a local NGO from the affected area will remain engaged because it is in its long-term interest to develop that area faster and better. Though committees are formed at the national level comprising all ministries, ultimately decisions will be made by the local people.

A workshop participant responded that perhaps local people may not have a very good decision making process. In most cities devastated in the Indian Ocean tsunami, people built their homes on the very same place, and the government is not stopping them. Kajla agreed that, typically, it is good to suggest that people rebuild in safer areas away from the water, but many will eventually return to their original location because they have no other place to go, there is a source of employment on the water, and they do not like to be far from their fishing boats.

THE CHALLENGES OF CONVENTIONAL TERRORISM

Technologies for Countering Terrorism

K. Sekhar framed his remarks in the context of significant changes in India that began after 9/11. There was recognition that terrorism, left-leaning ex-

tremism, insurgents, and people with various frustrations needed to be addressed more effectively. Given the Defense Research and Development Organization's (DRDO) research and development base, a decision was made to try to convert available technologies and to develop new technologies to help counter those threats more effectively with the singular objective of reducing the loss of lives. With this objective, a variety of paramilitary organizations were gathered to draft a program that identified the kinds of technologies that could be given immediately to fighting forces within a short period of time, approximately 6 months. It also addressed the questions: What are the technologies that can be customized over a period of 1 to 2 years and potentially be provided to the fighting forces? Within major, longer-term programs, where major technology breakthroughs might be made within 2 to 4 years? To address these questions, an assessment of possible threat scenarios is essential: The areas of vulnerability range from urban areas to forested areas, mountain regions, coastal areas, and desert areas. Indian air space is also vulnerable to infiltration by terrorists; hostage scenarios are of particular concern.

Sekhar listed recent terrorist events in India, including the 2008 Mumbai attacks and the landmine blast in Sandiwara, the Bengal blast, and the April 2010 Dantewada Maoist attack. In the process of examining these incidents and means of countering future terrorist attacks, Sekhar stated that efforts must start with surveillance and reconnaissance. For example, how can one improve the ability to fight at night, which is a particular challenge because most encounters with terrorists occur at night. Another challenge is establishing secure communications as well as gaining the ability to jam adversary communications. What kind of arms and ammunition are specifically required when engaging terrorists in open fighting? What are the nonlethal weapons that could be used to capture terrorists alive, and take them into custody for interrogation? Explosives detection and diffusion is also a very big challenge. One may detect an explosive; but diffusing it is more challenging. Personnel protection to support fighting forces and combat support systems are also necessary.

To address the surveillance and reconnaissance challenges, Sekhar stated that India already has developed a capability like the unmanned Nishant aerial vehicle that can be deployed, the Netra UAV, and the quadrotor helicopter, which is now being used very extensively by police personnel for crowd control, and battlefield surveillance radar, which can be used very effectively to control infiltration. Mountain radars, such as Bharani, also serve a similar purpose. Fixed-wing mini-UAVs are under development, and soon they will be operational.

Another immediate equipment challenge, especially in hostage scenarios, is through-wall imaging radar. The Israeli's have developed a radar that is being explored by Indian experts. It is not very effective, although it provides an idea of how many people are inside a building. Police would like more information about what is transpiring on the other side of the wall than can be obtained with technology today. DRDO asked a laboratory in Bangalore with expertise in radar to develop technology that can monitor the movement of people based on

their heartbeat and breathing patterns. This could distinguish very clearly, for example, among people who are moving and people who are seated. This is anticipated probably in a year or two. Through-wall emitting radar will be one of the first known radars for monitoring movements inside closed rooms. This would have been a considerable advantage had it been available during the Mumbai attacks. In conjunction, a "corner-firing weapon" would also be helpful. Similarly, multimode grenades are useful both for offense and for defense. Air-bursting grenades can be launched from a distance of 200 to 300 hundred meters and they can explode precisely at the desired altitude.

The topic of surveillance is something that India has been working on for quite some time. Balloon-based surveillance is valuable, especially in areas that are not easily accessible over land. India has had considerable discussion with some foreign countries, especially Sweden, to work with SAAB, a pioneer in foliage-penetration radar. India is also working to develop moving-target indication to detect people moving under the foliage. This is a big challenge in India, especially if one looks at the central part of the country. The movement of insurgents and left-leaning extremists takes place under these conditions; therefore, this could become a very important technological tool.

Sekhar noted that there has been a great deal of discussion in India about the detection of explosives. One of DRDO's laboratories, along with industry in Bangalore, is working on a point detector based on amplifying fluorescent polymers. They have demonstrated with many of the conventional explosives, like RDX, TNT, HMX, and PET, that even at very low levels of concentration, ppb-level detectors are sensitive to ammonium lactate. The major advantage with this type of detection is that it does not have a radioactive source and indicates the presence of explosives through a warning light. This technology is now ready, and within in 6 months to 1 year, it should be ready for deployment. Stand-off detection of explosives is another challenging area that many people have been working on, and another technology in development is based on laser photoacoustic spectroscopy, where the target is penetrated with tunable fiber-optic lasers, and the acoustic signal generated by the target is detected and analyzed. A sense of the target is gained based on the type of acoustic signals detected. This technology will likely take a few years to complete.

Left-wing extremists are a significant threat in central India. They have used hard-wired connection explosives rather than remote detonators and have laid wire for hundreds of meters and buried explosives at a depth of up to 2 meters. In some cases the explosives have been buried for months and years. Unless one has a method of detecting these explosives, there is always a risk. Terrorists see people coming and they sit about a hundred meters away physically connected to the explosive via hard wire. The moment people come to the point where the explosives are buried, the device can be detonated. To counter this threat, DRDO is trying to use well-known equipment called ground-penetrating radar, which is used to locate cables and pipes for construction activities. How can one effectively use ground-penetrating radar to detect explosives? DRDO's future plans include examining different kinds of explosives, different contain-

ers, different depths, different kinds of signals, and different kinds of materials. They will then prepare a large database with this information so that when an actual signal is detected in the field there is a greater likelihood of successful prediction of the actual kinds of explosives buried and at what depth. Sekhar hopes that in the next couple of years, they will be able to have a reliable databank.

Detection of the explosive is only the first step, however. After detection, how does one handle the explosive? Obviously one needs a remote vehicle, and India has developed a remotely operated vehicle called Daksh, which is capable of entering a building, climbing stairs, picking up an object and taking it to a safe place, and placing it down. Cameras and other equipment can also be mounted to the remotely operated vehicles. Then, having detected a significant amount of explosives, how should disposal occur? A laser ordinance disposal system was developed to address this challenge: using a laser beam, an explosive can be deflagrated at a distance of 50 meters.

Next, Sekhar explained, they examined communication systems to ensure that they are secure and also so that they can jam the adversaries' communication. They have developed an S-band mobile satellite terminal that is light weight (3 pounds) and that can be used anywhere. They have developed vehicle-mounted improvised explosive device jammers that have become a regular part of all BVA convoys in India. They have also developed a human-portable jammer so that people can enter areas not accessible by vehicles. In terms of acoustic eavesdropping, DRDO is developing technology to listen to conversations and detect the movement of terrorists hiding in forests or in remote buildings. They have developed a network of wireless acoustic sensor nodes placed over a large territory and then they are able to communicate to form networks. Significant intelligence capabilities have been incorporated into this network to have the ability to recognize specific voices. This technology is also in the process of being developed, and some positive results have been obtained. The nodes are able to communicate to a base station of the network, and the host at the base station conveys the communication to the control room. Should one or more nodes be damaged, the system will form another network and continue to communicate. Another technology is the optoelectronic-based eavesdropping system. With this technology, a laser beam is aimed at a suspected object like a window, and the voice inside modulates the laser beam, and the reflected beam provides an idea about the type of conversation. This has been successful up to approximately 20 meters in houses and cars, but the technology needs improvement so that it can be used for more applications over long distances.

Less lethal weapons are also very important, especially to flush out terrorists from hideouts. Oleoresin-based grenades were developed almost 6 or 7 years ago and are now being used extensively by India's ground forces, especially in the border areas where terrorists are known to be hiding. The CR-based tear gas grenade is an advanced version of a lachrymatory agent commonly known as tear gas. The advantage of CR gas is that it is less toxic, but more effective. Normally, one can protect oneself by placing a wet cloth over one's eyes and

nose; however, with CR gas a wet cloth aggravates the eyes and nose. CR will increasingly become a common element in tear gas.

Mine-protected vehicles are always being improved to make them as effective as possible. For example, today, Sekhar said, India is trying to develop vehicles capable of protecting people against explosions of up to 50 kilograms of TNT. However, the adversary may use 75 to 100 kilograms. This is why it is important to keep developing technologies, to send a strong message of confidence to the forces fighting the terrorists and to the terrorists about their capabilities. Also, bulletproof vehicles have become very important, and DRDO has developed vehicles that can withstand AK-47 fire as well as 7.2 SLR fire. Sekhar also noted the importance of personnel protection. Security forces need good bulletproof jackets. This was a serious issue during the Mumbai attacks because the armed forces, did not have the proper bulletproof jackets capable of giving them the required protection. With regard to chemical, biological, radiological, and nuclear emergencies, a nuclear-biological-chemical suit is essential. India has already developed such suits, and the armed forces are using them. Now they have developed a new version of the suit. Additional combat support includes life detectors for fighting forces. These detectors are sensitive acoustic detectors for people trapped under debris. If they can detect people, they can save lives.

Another incident that Sekhar touched upon was the Moscow hostage incident.[19] Fentanyl was used to incapacitate the terrorists, however the problem with fentanyl is that it is an anesthetic and hence the concentration levels are very important. Government forces pumped fentanyl through the air-conditioning ducts and people who were close to the ducts had much higher levels of exposure which caused casualties. In India, they have worked on gases equivalent to fentanyl, synthetic analogues, like remifentanil and carfentanil, which are much less lethal. The median lethal dose, or LD_{50} levels are much lower and are as effective as fentanyl. India is exploring different methods of dispersing this anesthetic, including UAVs, which look like birds. They are being positioned at various places where people congregate in large numbers. These vehicles will operate a valve and fentanyl can be dispersed, but the concentrations are much lower, avoiding casualties.

Finally, biosensors are being developed based on nanotechnology to detect biological and chemical agents. India hopes to develop sensors that are small and cost a few dollars that can be put in a number of areas around sensitive points. If there is an attack, these sensors will detect the type of agent that has been used, at what time, and in what concentrations. This will enable proper protective measures and counter-measures.

[19]Krechetnikov, Artem. "Moscow Theatre Siege: Questions Remain Unanswered." *BBC News*, October 24, 2012. Available at: http://www.bbc.com/news/world-europe-20067384; accessed October 20, 2014.

Sekhar concluded by stating that if they can accomplish these tasks, they can protect sensitive installations from chemical and biological attacks. India can collaborate with other interested nations to enhance the combat readiness and effectiveness of forces engaged in countering terrorism.

Developing Comprehensive Training for Future Explosives Experts

Byron Gardner spoke about security at globally strategic facilities—nuclear, chemical, energy, and liquid fuel—and incidents that can have a significant impact on the national security of a country or on global security. The problem he said is that many of the security systems are not integrated and they do not work. In the United States, there have been some incredible mistakes at the Department of Defense, the Nuclear Regulatory Commission, at nuclear power reactors, and at the Department of Energy (DOE). Gardner has had the opportunity to work on some of the world's most important facilities, and he finds these problems everywhere.

During his presentation, Gardner proposed a solution to these problems: to ensure that security professionals really understand the problem from a system engineer's perspective, which they often do not. People managing security systems or major facilities tend to be in one of two categories. They are exceptional policeman, have had great experience and are placed in a high-security job, or they are exceptional people from the facility itself and yet they do not have a systems engineering background to run all of the complex systems that are under their jurisdiction.

To begin, Gardner provided a summary of the problem. Brand new, multimillion dollar security systems have failed during attacks or performance tests. These systems typically cost around $10,000 per meter to install and operate around sensitive facilities. That is expensive when perimeters are a couple of miles long. These systems are designed and installed in full compliance with government regulations, including double fences, cameras, lights, and alarms, but when they are tested often they do not work, and in some cases when terrorists attack, the alarm does not sound. Why not?

High-technology systems are rarely integrated, although these kinds of systems should be synergistic. The alarm systems should generate an assessment that in turn generates a response that is able to neutralize terrorists before they can destroy the target. If the alarm systems are not integrated, one piece might work, but the system itself does not work. A large part of the problem is that humans have to be involved in the system; however, there is pressure to take humans out of the loop. In Gardner's opinion, that is a big mistake. Facility operators usually do not understand the capabilities and limitations of the security systems. That includes the government and system operators. There is an absence of design basis threat in many critical industries. United States critical energy facilities have security systems designed to prevent the theft of steel and copper, but not to prevent sabotage that may shut the power off to major regions

of the country. Further, systems are often installed that do not take into consideration the environment in which they are operating: it makes a difference whether the environment is hot, cold, snowy, or windy. Security vendors will sell anything, and they will say a piece of equipment works and charge a lot of money, although it might not perform as expected. Further, systems are often not installed and maintained properly.

Gardner's assessment of the problem is that the people running these facilities lack hands-on experience, and it takes many years before people are fully productive. Security management professionals and government oversight inspectors often do not understand much of the new equipment; rather some feel that if they spend the money, everything is going to be fine. Further, the high-security expertise needed to run integrated systems, at least in the United States, does not reside in one institution, whether it is colleges or universities or national laboratories. Therefore, Gardner and his colleagues attempted to create a security program at Arizona State University and New Mexico State University, mainly based on good textbooks, but it failed because they did not incorporate the practical side of security requirements.

Traditional industrial security solutions do not work for major energy facilities and their support elements, whether it is power generation, desalination, or liquid fuel transport. The threat is great: terrorists may cause horrible, catastrophic consequences to economies or kill many people. The other issue that security management often does not understand is that cyberdistributive control systems and supervisory control and data acquisition (SCADA) threats are truly out there. Many security managers do not understand anything about cybersecurity of SCADA networks, therefore it is just pushed off to another organization and not integrated and as a result the systems do not talk to each other. Too often the perception is that kids are hacking in a basement, but there are vulnerabilities of a combined cyber and kinetic attack or physical attack.

Gardner then provided some examples of systems that cost on the order of $50 million each. He showed a perimeter along a globally strategic facility. The assessment zone is about 400 meters long and to adequately determine if someone is penetrating a facility, ideally it should be about 100 meters long. Therefore, if someone crosses over that facility, guards too often ignore the alarm. In an exercise, Gardner recounted that six people went across a perimeter, and the command center could not tell what was happening. In another example, the system was installed improperly, resulting in the inability for security personnel to see the perimeter clearly and to see if anyone was hiding. Typically, if someone runs across an alarm zone, unless there is a pre-alarm recording, an intruder can actually hide within the zone before someone sees him or her. The alarm might go off and by the time the operator puts down his or her work and looks at the screen, the intruder may be off the screen; therefore, the operator does not see anything and declares the incident a false alarm. At another globally strategic facility, a brand new, $50 million security system was installed, but the operator could not see what was going on in the area under observation because the lights were not installed properly. Another problem that occurs all over the

world has to do with vehicle barriers. Sometimes a trench will be put around a facility but still have a high avenue of approach; therefore, even with a nice big trench, a regular Toyota can just jump across it. At another facility, Gardner recounted that a new, $50 million security system was installed with a vehicle barrier at the entrance but not at the exit.

In the United States, "Jersey barriers" (cement obstacles) are often placed around government buildings, diplomatic facilities, and nuclear and chemical facilities. If a vehicle hits the barrier driving fast, the vehicle will be destroyed, but if a heavy truck just pushes on the barrier, it will easily be moved out of the way and the truck can drive right into the facility. That is common. In yet another case, people just drove right through the trees. Gardner provided another example where the physical barriers are outside of the alarm area. There is no benefit to delaying a terrorist if there is no detection beforehand. In this case, the vehicle barriers and the concertina wire are outside and the sensors are inside and if they go off, the terrorist is already running up to destroy the target. Still another common problem is that the security forces are deployed at the main gates, and their security commanders often say, it is impossible for terrorists to go over our fences because we have concertina wire. However, a person with good clothing hopped over a fence with concertina wire in about 11 seconds. This often causes the site commander to acknowledge that they need to change the response plan. Yet another $50 million security system had a good drainage ditch coming out of the facility and a terrorist could enter through the drainage ditch, go right underneath the security system, and pop up inside the facility.

Another common problem involves vibration cables on fences, but if they are installed in a windy area the alarms sound all the time. At another $50 or $60 million facility, with alarm-system vibration and fiber-optic vibrations, a sturdy ladder for a terrorist to climb up was placed against the wall so that the cable would not vibrate; a terrorist could crawl right over without an alarm sounding. In another case, a brand new, $50 million system had 3,000 alarms in 3 days. Do you think the guards will assess an alarm and respond to it in these conditions? They just turn the alarm off. One can throw all of those millions of dollars away. With another example, Gardner explained that there is a maritime nexus to many facilities, such as ports or critical energy facilities. These systems need to be tested as well. Gardner showed an example of a performance test team swimming up to a sensor, swimming around it, and banging on it with a wrench, and it did not go off. This was a brand new, multimillion dollar system. What was wrong? Someone did not know how to performance test the system.

What is the solution? For Tier-I, priority A, globally strategic, very important facilities, we have to do something to kick-start an awareness of how these systems should run so that governments and private industries do not waste money and create vulnerabilities that could affect our societies. Gardner said that it baffles him as to why 50-kilovolt transformers and the radiators that support them are not hardened. Not many transformers are made in the world, but the new ones that are made should have ballistic hardening that is oriented to

where they could be vulnerable in order to render standoff attacks from the outside ineffective.

Effective systems analysis involves response forces, deployment, and equipment. There is a tremendous propensity in the security industry to ignore the guards. Many believe that if they buy fancy equipment, the guards will respond. However, guards have to be integrated as well. Security systems inspections and evaluation are also critical. The Y-12 National Security Complex incident was, in Gardner's view, a result of a weakened inspection program that did not have anyone trying to maintain awareness of what was happening.[20]

Gardner and his colleagues are trying to create a multidisciplinary, rotational graduate internship program to target early-career government and industry personnel. The program will cover issues that professionals need to know to question what is occurring in their facilities. Topics will include sensor and equipment security evaluation and testing, ballistic protection and critical infrastructure components. There is an agreement among several entities to create the multi-disciplinary program Gardner and his colleagues envision. The first one is Lawrence Livermore National Laboratory (LLNL). Experts at LLNL would discuss systems effectiveness, meaning vulnerability analysis; emergency preparedness and response, response force training and industrial security operations. Sandia National Laboratory (SNL) is going to be a part of the program and teach how to evaluate sensors, how to test them, how to look at the environmental conditions, and then they are going to have part of the National SCADA Test Bed Program that will allow people to actually gain some hands-on experience with cybersecurity. Texas A&M Transportation Institute will do live, full-scale vehicle crash tests with this group of students, and every rotation will do their own crash test. Then they will also go through emergency preparedness training at Texas A&M. Each rotation of students will be able to put blast waves across an infrastructure of interest to their industry or their country and also perform ballistic penetration tests on infrastructure. A theme running through this course is the idea that students will be able to understand the physics requirements, and be able to evaluate how to procure, maintain, and operate a security system that will provide the necessary protection. A utility company in California, Pacific Gas and Electric, will also participate in the program and provide training on industrial security planning and emergency preparedness. Pacific Northwest National Laboratory (PNNL) will provide training on industrial safety and cybersecurity, and then they will provide an instructional block on maritime security. Carnegie Mellon's Computer Emergency Response Team, will provide an instructional block on cyberdefense.

In a 1-year rotation, students will go to LLNL for an introduction with all the national labs and then they will split into groups and rotate to SNL, New

[20]See, for example, U.S. Department of Energy, Office of Inspector General, Office of Audits and Inspections. *Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*. Special Report, August 2012. Available at: http://energy.gov/sites/prod/files/IG-0868_0.pdf; accessed September 25, 2014.

Mexico Tech, Texas A&M, and PNNL. They will go on field trips to the Strategic Petroleum Reserve and the DOE National Training Center, and they will have a block of instruction on response-force training for Tier-I facilities. They will also visit U.S. Coast Guard facilities and attend the American Society of Industrial Security conference. They will write a thesis at the end of the program and will be evaluated by their own country or by the United States.

Gardner and his colleagues want participants to receive certification and accreditation for the course, and both New Mexico Tech and Texas A&M are very interested in providing certification for the entire program. The program will be implemented on a pilot basis initially, with 20 participants from the United States and other countries. The first pilot program is just about to be funded. Gardner ended by saying that hopefully the program will start having an impact. It is just a start, but these facilities are too important, and the impact on the global economy, and maybe hundreds of thousands of lives, is just too important to delay.

DISCUSSION

S. Gopal opened the discussion by asking Gardner to clarify if the cost of $50 million for security systems included the cost of the equipment. Gardner said that the cost included equipment purchase and installation. Gopal said that normally one conducts performance assessment trials before such very expensive equipment is purchased. Gardner replied that Gopal's question gets to the crux of the problem. The questions are: How does it happen that after the equipment is purchased and installed, there are performance problems? Why does the system not work? Do the checkout procedures match what the threat should be? How should the systems be performance tested? This requires not just a functionality check, but an actual performance test. Does the alarm system allow for an assessment in sufficient time to generate a response that can actually interrupt the adversary to keep sabotage from occurring?

An Indian participant recalled his experience at an ammonium plant three decades ago. Although they had very good tools, the operators received a flood of alarms because there were so many signals triggering the alarms to go off, and the net result was that guards ignored the alarms. Now Windows is starting to supply alarm management software; however, technology that one does not understand is by itself a threat.

Gardner was then asked about the cost of the graduate program. He replied that it is not as expensive as one might think. It is as expensive as a regular graduate program, but the universities will charge the tuition rate for a 9-hour class for each rotation. The universities are much more cost effective than the labs: A full-scale vehicle crash test for Texas A&M is about $40,000, including the truck and all the instrumentation that goes along with it. The explosive training at New Mexico Tech is nearly free, and the university is providing a range to do it. Finally, salaries are another expense. Salaries at the national labs are high, and the program has a couple of experienced people as mentors. Further, one

may believe that this type of program is sensitive from a security perspective, but as long as we are using infrastructure that is generic worldwide or applicable to the country or industry of interest, the U.S. Department of State has approved the program.

A workshop participant asked about cooperation with industry through the program and the agenda of industry in participating. Gardner replied that the goal is to inform the management of facilities and those who provide government oversight that security and therefore the training has to address the problems and perform to address these problems. The program is a great first step for cooperation with industry. This could really be a good way to have some cooperation across these Tier-I industries and across countries. For example, the United States has trouble with its southern border with Mexico. High-tech sensors were installed and a great deal of money has been spent, but the problem still is not solved, because people still have not grasped the problem fully.

John Holmes added that, having accepted many security systems that were not functional, in many cases the problem is that testing has been done on pieces of the system and not the whole system. Often part of the system is finished and tested, and then the next part of the system is finished and tested. Sometimes the full system is never functionally tested. Also the people accepting these systems are not necessarily professionals in that area of security, and performance testing is a very complex issue. Therefore, if the person who makes a test plan is not familiar with performance testing, sometimes the system is less than functional because the person does not know how to test the entire system properly. Holmes worked with the U.S. National Academy of Sciences on several projects, and he came to understand this challenge much better. This is a very specific area of study.

Gardner agreed and added that this is why the program he described includes 2½ months of performance testing. Although the facility manager is not personally going to be doing performance testing, he or she needs to be available to evaluate the test plan, observe it, and ensure that the security system is working.

6

Learning and Applying Best Practices to Counter Terrorism

CASE STUDIES FROM INDIA AND THE UNITED STATES

Screening of Documentary Films

In addition to presentations and discussions, workshop participants also viewed two films: *Terror in Mumbai,*[1] and *Manhunt – Boston Bombers*.[2] The first of the documentaries provided video footage, audio recordings taken as the events unfolded, and subsequent analysis of the November 2008 terrorist attacks in Mumbai that were perpetrated by a group of men who came from Pakistan. The second of the documentaries provided videos and audio reccordings as well as analysis of the events surrounding the detonation of two bombs during the Boston Marathon on April 25, 2013.

On November 26, 2008, the terrorist group Lashkar-e-Taiba, the Army of the Righteous, launched a multiple-site attack on Mumbai that was "to stage a spectacle so terrifying that the world could no longer ignore (the group)." *Terror in Mumbai* opened with audio recordings of cell phone intercepts of the terrorists and those from whom they were receiving instructions in Pakistan: "You're very close to heaven. For your mission to end successfully, you must be killed. God willing. … The enemy must fear us. When this is over, there will be much more fear in the world." As the attack proceeded, a controller in Pakistan asked one of the terrorists, "How many people did you kill?" to which the young man answered, "I don't know. Kept firing and firing." According to the film, undercover Indian agents had previously provided 35 SIM cards to the Pakistani terrorist group, and intelligence officers discovered that three of the SIM cards had been activated the night of the attack, which allowed them to listen in on a total of 284 calls.

[1] *Terror in Mumbai*. Transcript. HBO Documentary Films. Aired 25, 2012. Available at: http://transcripts.cnn.com/TRANSCRIPTS/1211/25/se.01.html; accessed September 16, 2014.

[2] *Manhunt-Boston Bombers*. Transcript. NOVA video. Aired May 29, 2013 on Public Broadcasting Service. Available at: http://www.pbs.org/wgbh/nova/tech/manhunt-boston-bombers.html; accessed on September 16, 2014.

Most of the calls involved a single controller identified as brother Wasi and the terrorists on the ground. During one such intercepted call, Wasi directed the terrorists to, "Pile up the carpets and mattresses from the room you've opened. Douse them in alcohol and set them alight. Get a couple of floors burning. And when we ring, make sure you answer." The next call was to check on progress: "Have you started the fire yet?" "No, we haven't started the fire yet." "You must start the fire now. Nothing is going to happen until you start the fire. When people see the flames, they will start to be afraid."

Throughout the frightening three days, the Mumbai police force and Indian officials listened to the terrorists' calls and tried to stop the killing and end the attacks. An unidentified Indian official stated that they were not prepared for the multitude and complexity of the attack: "We are used to a blast occurring. We go to the spot, clear the area, sanitize the area, collect evidence and begin our investigation. … We were prepared for a terrorist strike, but maybe at one location. Four or five locations simultaneously, then going into hotels and taking hotels, all these things contributed to… making the situation a very, very difficult one." Although the intercepts of the calls were a significant contribution, opportunities remain for science and technology to further strengthen prevention, response, and investigatory capabilities in India.

The Boston Marathon bombings, conversely, were a single-point, daylight attack, staged at the finish line of the annual race where medical personnel and equipment were pre-staged to assist runners who may need help after having run the full 26 miles. These circumstances assisted first responders, police officials, and investigators in treating the injured quickly and in determining the cause of the blasts within a short period of time. Locating the people who set off the bombs, however, proved to be more difficult and required several days of police and detective work coupled with outreach to the public.

Rather than a lack of evidence, investigators had a significant cache of videos, photos, and physical debris to aid their efforts. Sifting through the volume of material available as quickly and thoroughly as possible proved a considerable challenge. Workshop participant Van Romero was interviewed in the film, *Manhunt-Boston Bombers*: "I started looking for broken windows. That tells me where the pressure rate was and how big the pressure rate was. Is there a crater? All that analytical stuff is going through the brain." He also observed white smoke, which is a "surefire sign of a gunpowder explosion. It means the devices are likely homemade."

In addition to large amounts of physical evidence, perhaps the key to identifying and ultimately locating the suspects was access to several videos from surveillance cameras at the scene. Boston Police Department Superintendent Bill Evans, interviewed in the film, knew that there would be good video, but "Detectives must go door to door, hunting for visual evidence, since the cameras are privately owned and individually monitored. Boston only has a limited number of cameras, and there is nothing tying them together. Each video will have to be collected and viewed separately, a laborious and time-consuming process." In addition to videos from surveillance cameras, officials asked the public to sub-

mit their personal videos as well, which they did in large numbers, creating another considerable amount of footage to screen. While there is some facial recognition technology available, Evans stated, "in this case, it didn't help us that (much). The FBI didn't know who these suspects were." While investigators were pouring over the videos and pictures, people were releasing their own videos and photos online, which meant that "innocent people were being fingered for a horrible, horrible crime, and that was putting those people at risk." Given the fact that innocent people were being accused, the FBI then released photos of the actual suspects to the public to seek their assistance.

Ultimately, the technology that helped break the case and led investigators to the suspects was the tracking of a cell phone left in the car that was hijacked by the suspects. The hijacked driver was able to escape and to contact the police and they traced the phone and the car in which the phone was riding and tracked down the suspects. Although one suspect (Tamerlan Tsarneav) was killed in that encounter with the police, the other suspect (Dzhokhar Tsarnaev) fled. Again, a break in the case came from a citizen who identified blood on the boat in her backyard and notified police. Using a helicopter carrying a thermal camera, which "can detect even subtle temperature changes," investigators confirmed the location of the second suspect and apprehended him. Throughout the initial response, the detailed investigation, and the capture of the surviving suspect, technology aided investigators, but it did not solve the case on its own. Humans watched hours of videos and looked at thousands of pictures, experts walked painstakingly through the crime scene, detectives went door to door, and citizens responded rapidly to key events. Together, people, with the assistance of technology, succeeded in ending the search for the Boston Marathon bombers within days. Much more work needs to be done to improve the technologies that can aid those involved in responses to such complex attacks.

Experiences of Science and Technology to Counter Terrorism: Incidents in India

Keshav Kumar summarized the knowledge he has gained through hands-on experience utilizing forensic science in criminal investigations. He addressed forensic capabilities during response phases, attribution, and prosecution, as well as current capabilities in India and innovative technologies around the world. Finally, he addressed how coordination between the United States and India may be forged.

Kumar noted that an entire investigation is often based on Locard's principle of exchange, which states that when two objects come into contact, there is a transfer of material between them.[3] Through the material transferred, Kumar connects the crime, the criminal, and the victim. He connects the scene of the

[3]Department of Emergency Services and Public Protection, State of Connecticut. "Forensic Biology." Available at ttp://www.ct.gov/despp/cwp/view.asp?a=4154&q=487944; accessed October 20, 2014.

crime, the physical evidence, and the victim through scientifically-collected forensic evidence.

Forensics is important for prevention, detection, and conviction. Prevention is proactive forensics, which is essential for counterterrorism, and which Kumar feels is perhaps the most important of the three. How might technology help prevent these incidents? What are preventive forensics and proactive forensics? Rather than conducting a retrospective analysis of an incident that has already occurred, the idea of proactive forensics is to look for threats in advance, using known characteristics of terrorist activities to identify intended attacks before they happen. If one can collect forensic intelligence, an incident might be prevented by using analysis and detection to make a forensic databank with a multitude of variables.

Kumar then walked through a classic case of a bomb explosion crime scene and how forensics can play a major role in the postblast investigation. Reconstruction of the incident, establishment of the actual site of the explosion, the collection of various clues, and a search for any live explosive material are critical elements. Kumar asks, what kind of explosive was used? How much explosive was used? How was it detonated? How many people were killed and injured? These are elements of the bomb signature sought by forensic investigators. Photographs are helpful in investigating explosions to identify the type of bomb and the bomb signature. Other evidence from the scene of the crime includes bullets and rivets. With improvised explosive devices (IEDs), forensic experts look for bomb components, initiators, and detonators. Kumar then noted that some terrorists use mobile phones to detonate IEDs. Forensic scientists can examine and analyze batteries and electric wires. India has frequent pipe bomb incidents, such as recent incidents on city buses. Evidence at each site provides a signature of the particular perpetrators. What can one possibly know about the explosive signature? Particular types of containers, wrappings, fuses, or circuits are often specific to a particular group.

Sniffer dogs have a smelling capacity that is 40 times that of human beings. They hear 20 times more than human beings, and their vision is 10 times better than human beings. Given their abilities, sniffer dogs can be helpful at postdetonation blast-scene investigations, particularly in combination with detection technologies.

Other pieces of evidence include blast-caused smoke residue. When explosives burn, they emit some type of colored smoke that can indicate that a particular type of explosive was used. Explosions often leave traces that can be found on hands, clothes, pockets, fingernails, under rings, or in skin creases. Some countries have also been using taggants in certain kinds of explosives. With this evidence, Kumar may be able to identify the explosives manufacturer and/or the batch of the explosive material. This may provide an indication of the people involved.

Kumar then turned to DNA profiling. DNA has recently been given a great deal of credibility in investigations and is possibly a 99.99 percent foolproof type of forensic evidence collected at any incident sites. What evidence

can we get at the scene of a crime? Biological evidence can be extracted from many sources—fingerprints themselves and trace DNA extracted from fingerprints are sources, as well as the DNA collected from anything that has contact with the body, like a toothbrush. Body fluids on shirts and other clothing can be good sources of evidence, as can documents and disposable cups. In all of Kumar's investigations, he has used physical evidence and trace DNA. In his experience, the Honorable Court has appreciated the value of the forensic evidence. In one of the investigations in which Kumar participated, the defendants were not released on bail due to the forensic evidence collected against them, including DNA.

New techniques are under development: facial reconstruction based on DNA to identify possible suspects is an area of active research in the United States and elsewhere. These technologies could be coupled with 3-D printers, and this could change the dynamic of counter terrorism. India already conducts facial reconstruction from skulls. Audio-video forensic analysis is a new technique focusing on voice dynamics and voice templates. Kumar suggests having a databank of all the voice samples from intercepts for later comparison. Software can enhance the signal in a low-quality recording, and this has been used for closed-circuit TV surveillance. Kumar also mentioned psychological forensic tools, such as polygraph and other interrogation verification tools, like "brain fingerprinting," delayed voice analysis, and behavioral profiling of people at airports.

He suggested that development of certain capabilities would be useful, including: non-lethal incapacitation technologies; real-time friend-or-foe identification during incidents; and remote observation of crime scenes by a team of experts (India is already doing this in Gujarat). How, he asked, can we have an international coordination mechanism in the fields of capacity building, research and development, best practices, training of forensic scientists, and gadgetry enhancement? Interpol could be a useful mechanism. Kumar closed by saying that the legal aspects also need to be examined for all of these tools.

The Boston Marathon Attacks

Van Romero, featured in *Manhunt-Boston Bombers*, opened his remarks by stating that in footage of the Boston Marathon attacks, one can quickly see that there is data everywhere: white smoke, for example, is seen right away. One can also see the second detonation, which is a really important piece of information for trying to understand what happened. Romero knew of no other event that had as much video, as many pictures, and so much evidence to aid the investigation. The problem however, was paralysis by analysis. If one has too much data, it can be overwhelming. The authorities in this case did an outstanding job of digging, drilling down, and using the data that was important for the investigation. They also were lucky, but they knew how to shape their luck as time went on.

At 2:50 p.m. on April 15, 2013, the devices detonated and three people were killed. Investigators knew right away that there were two devices and that they detonated approximately 10 to 15 seconds apart, which certainly indicates good coordination and some degree of sophistication. The city of Boston in the state of Massachusetts has spent money and a tremendous amount of effort on training and was well prepared to respond to incidents such as this. There were several other aspects that put them in a good position to deal with this incident. Given that the targeted event was an athletic event with many participants, there were a lot of medical staff on hand right at the finish line, so all the people that were needed were pre-positioned to respond. Also, the responders had been trained to respond to these types of explosives incidents, 1,500 people from Boston had been trained at New Mexico Tech to respond to a terrorist event like the one that occurred at the Boston Marathon.

The first element of a response effort like this is to transport a large number of people to hospitals, and as a result, this process may become a secondary target. In these cases, it is important to continue to protect the injured, but the suspect(s) may also be transported with the victims. It may not be clear that one of the injured may also be a perpetrator, so security at the hospital becomes very important. Boston authorities did a good job of establishing security at the trauma centers where people were being treated. An important lesson learned is that the day is not over just because the bombs have detonated. There could be something else happening, and one has to examine the entire situation fully.

After the victims had been transported from the scene of the detonations in Boston, the scene started to calm down, and the investigation began. Everyone wanted data as quickly as possible, and the situation was very dynamic. The entire investigation of the event took place over 5 days. Meanwhile, there were still potential hazards at the crime scene. There could have been secondary devices planted by the terrorists, and there were natural hazards such as falling glass; training on how to deal with crime scenes is important. Romero explained that the second bomb was about 600 feet away from the first bomb. Before the attack, surveillance cameras captured the two suspects coming around the corner, walking onto Boylston Street together. One of them stopped in front of the Forum Restaurant and the other stopped farther down the street. When the first bomb detonated, there were broken windows and victims were hit by debris and shrapnel from the bomb. Thirteen seconds later, the second bomb detonated. It did not hurt as many people because people had already been alerted to the fact that something bad was happening and they started to take cover. After the attack, video footage indicates that the suspects fled and went back the way they came. Investigators had this data and were trying to identify these people.

There was an enormous amount of data, and because there was no automated system for sorting through it (New York City is the only city that has this process automated), the investigators spent a tremendous amount of effort in a very short period of time combing through all the video recordings and isolating where the suspects might be. It was just good, old-fashioned, hard police work.

Early investigation of the IEDs indicated that they were 6-liter pressure cookers and they were in backpacks carried by the suspects to the site. Based on reports from the scene, the IEDs each likely consisted of a pressure cooker with low-level explosives. The pressure cookers also had been packed with nails and BBs as shrapnel. The white smoke and the gun powder is evidence of the presence of gunpowder ignited by an electrical fuse. The explosive material was taken from commercial fireworks. How were the devices detonated? Based on the evidence quickly recovered at the scene, it is likely that the IEDs had electronic fusing systems. There were transmitters and receivers installed so that they could be triggered, essentially like pulling the trigger on a gun. The suspects used electronic speed controllers, and batteries were found at the scene along with the receiver that was in the device. Some of the circuitry was also recovered at the scene. This evidence can only be recovered through hard work, as people meticulously combing through the evidence. The conclusion is that the suspects used remote controllers for children's toys, which are used to power cars that race around on the floor. They usually operate in the megahertz range and one can pull the trigger and wirelessly control something at a distance. Typical distances for these types of controllers are between 50 feet for a lower-end toy to about 1,000 feet for a hobby-grade device. A remote controller can easily be hidden on a body or in a backpack. One could walk perhaps 1,000 feet from the device, detonate the first bomb and then pull a trigger to detonate the second bomb. While this is fairly simple, it does indicate some degree of sophistication, and probably some training. Inside the pressure cooker, black gunpowder was surrounded by some sort of shrapnel. An electric match was placed inside the black gunpowder, so when a switch was flipped, it started to glow or burn and that ignited the gunpowder, which blasted the cooker apart and sprayed the shrapnel.

Romero then described how he and his colleagues study pressure-cooker bombs. They lay the pressure cooker on its side so that the lid and the bottom go through what they call "witness plates," because they want to see the trajectory of the explosion and to be able to measure its velocity. In reality, one of the pressure cookers at the Boston Marathon was probably set up vertically because one lid was found on top of a building, so it was probably launched. During a test of a pressure-cooker bomb set up vertically, the lid went straight up and came straight back down. Romero showed a comparison of a pressure-cooker lid after an experiment and one from the Boston crime scene. There is a striking similarity when one examines the lids of the pressure cookers. After approximately four or five tests, Romero and his colleagues found that the results they obtained were identical.

Other people have used these same types of pressure-cooker bombs. There was an attempted bombing in Times Square in New York City. An alert person saw the vehicle and thwarted that bombing attempt. There was a similar event at Fort Hood in the United States, where there was a plot to use a pressure-cooker bomb against soldiers. Romero tends to see a lot more pipe bombs in the United States than these types of pressure-cooker bombs, but these types of pressure-

cooker bombs are much more prevalent in South Asia, perhaps because pressure cookers are used more often to cook food, which means they are readily available.

With regard to explosives, the gunpowder used in the Boston bombings was obtained by purchasing fireworks, but fertilizers can also be used for bombs and urine can be used to make urea nitrate. These are all very common items that one can possess legally, and so it is difficult to trace where they come from and that makes part of the forensics job tougher.

The release of the suspects' photos was a significant turning point in the whole investigation. There was a lot of discussion as to how law enforcement would start to reveal this data to the public. In today's environment, constant news reporting also creates a great deal of false reporting. There was also social media that lit up with this story, and Romero believes the correct decision was made by law enforcement to share the suspects' photos with the public because photos were being disseminated anyway, and law enforcement wanted to state explicitly what they were looking for. That led to the chain of events that resulted in the capture of one suspect and the death of another. There was tremendous community participation as well, which was very important to remember. Essentially, one part of Boston was locked down, and the civilian population was amenable. People paid attention and did what they were asked to do. The citizenry in the affected area did a very good job of following the guidance of law enforcement: They sheltered in place, became vigilant, and reported anything out of the ordinary. A citizen report was the final break that led to the use of an infrared camera that identified the second suspect.

One of the messages that Romero emphasized was that when he looks at an integrated systems-level response, one has to consider the human aspect as well. Humans are a very important aspect of making the system work. Just because one has technology does not mean the problems are solved. Training personnel is important. The importance of the collection of information and strategies for analysis cannot be overstated. Terrorists will continue to evolve, and they will interact with the public, and our ability to stop them is paramount.

DISCUSSION

A participant asked how decisions are made concerning tradeoffs between preservation and collection of evidence on the one hand and addressing the immediate needs of the victims on the other. Kumar replied that in each state of India the police force is independent. The National Investigation Agency has the power to take over some investigations. **Byron Gardner** noted that at a crime scene, in the United States there are other responders—the police, firefighters, and medical response personnel—and it is important for the responders to train together so that, for example, the firefighters do not wash away the evidence.

Another participant raised the issue of the credibility of types of evidence in India. An Indian participating noted that brain mapping or brain fingerprinting is controversial, and not viewed as reliable and is therefore not admissible in

courts. Kumar noted that all of the aids to investigations he mentioned—polygraphs, for example—are of no evidentiary value, but the courts may interpret them how they choose. All of the judges in Gujarat, for example, are now undergoing training in forensics, which helps.

The same participant also noted that there are many reasons why someone in an airport may be under stress, so stress is a poor indicator of terrorist intent. Kumar agreed and said that this is why there needs to be good coordination between man and machine. The operator needs to evaluate the actual situation.

Kumar noted that as far as capacity building goes, progress is very slow. Of late, the best possible forensic lab in India is in Gujarat, and none of the forensic labs, even the central labs, can compare with the forensic capabilities in Gujarat. This is most likely due to the proactive approach of the director of forensic science there. This laboratory serves as a good model and does analysis for others across the country. However, this analysis is expensive. Payment received for the analysis is split, with 50 percent going to the government and 50 percent going to the laboratory to be spent at the discretion of the director, so at any given point the director of forensics has sufficient financial resources, and whenever new technology is needed he is in a position to acquire it. As an example, software for audio and video authentication and enhancement is available only at Gujarat. None of the state forensic science labs or even the central ones could spend so much money on software. Therefore, while capacity building is taking place, it is on an individual level, and international cooperation on forensics could be especially valuable. Kumar personally feels that India can bring significant expertise to research and development (R&D) collaboration. This type of cooperation would be mutually beneficial to India and the United States.

Romero responded to a question about public acceptance in the United States of data collection via surveillance cameras. Many people have accepted surveillance as consumers when we go into stores, but we do not realize that at some point that store video may be used by the Federal Bureau of Investigation (FBI). We have grown accustomed to having these cameras in many different locations. However, once an event happens, the public becomes very good about collaborating with law enforcement under a stressful situation. There are people who worry about civil liberties, and it is important for them to do so, but under extreme circumstances, many people are helpful and even volunteer data. Data is also collected by private companies and private businesses. This data belongs to the businesses, but they are often willing to provide it to law enforcement.

With regard to wireless connections, New York City has a tremendously powerful tool for integrating information from many sources, but it was expensive. Real-time collection is important, but terrorists could easily tap into private data collection and corrupt the system. Romero added that exercises are vital for bringing all of the appropriate people together and putting them in the roles that they are supposed to play so that they can understand how everything works in an incident control center. It is important to follow the National Incident Management System (NIMS) hierarchy so that the chain of command is well understood. The United States has a long history of poor coordination between the

FBI and local law enforcement, but that has largely been overcome. In the United States, the FBI has jurisdiction over cases of terrorism.

Micah Lowenthal contributed two comments. The Boston Marathon case shows how far we have to go in the technology arena. The law enforcement response does not necessarily show what technology enables us to do; it shows how, in some cases, it is not as useful. The most important breakthroughs in the Boston case in terms of catching the suspects came from the hard work that went into finding those photos and releasing them. The person in the community who was carjacked escaped and called the police immediately, and thereby provided a big break. Technology figured into finding the cell phone that was on, and into training the helicopter-mounted infrared cameras on a parked boat to confirm that a person was hiding there. But the infrared cameras did not find the suspect until a resident called in to report blood on her boat. The technologies are totally irrelevant until someone says, "look here," because they have a tremendous amount of data and no information. Therefore, we have a long way to go.

Romero added that it took a couple of lucky breaks for the capture to have been successful, but he believes that one makes one's own luck. The law enforcement in this case was doing the hard work of sifting through all that data and had positioned themselves so that when those breaks occurred they could take advantage of them. One cannot just sit back and let the breaks happen.

Lowenthal raised another point, there are many tools out there, but they are not always effective. A recent National Academy of Sciences report, *Strengthening Forensic Science in the United States* caused the country to reexamine all of the traditional techniques that have been used in forensic science much more closely, because it shows that the scientific basis for these techniques had not been established.[4] This does not necessarily mean that they were wrong, but we do not know how reliable they are. These technologies range from tool marks to bite marks to fingerprints, bullet lead composition, and a whole host of methods. There is an effort now in the United States to reexamine them and try to establish a scientific basis. Are there any such efforts in India and other places?

Kumar replied that in India there are a number of circumstances that have caused reconsideration of these techniques, the latest being a Supreme Court judgment that challenged scientific investigations through polygraphs, fingerprinting, and so forth. One cannot subject a person without his or her informed consent to certain techniques, and there is now a limitation on all of them. As far as the reliability of the tests goes, Kumar believes that with the passage of time and with R&D, in approximately 5 years we will again challenge what we are thinking now. With regard to DNA fingerprinting, the number of base pairs that are required to give a proper shape is also questionable. Today we are basing it on 13 pairs, but perhaps tomorrow one can go to 15. With the rapid advance-

[4]National Resarch Council. Committee on Identifying the Needs of the Forensic Sciences Community. *Strengthening Forensic Science in the United States*. Washington, D.C.: The National Academies Press, 2009.

ments in science and technology, we will surely challenge what was done earlier. The judiciary needs to be made aware of these developments so that there can be coordination between all three branches of government. Only then will they be able to appreciate the forensic evidence in a holistic fashion. Romero noted that in a trial, one has to convince a jury of common people, not a scientist or a forensic investigator, that the data convicts the accused person. That is difficult to do.

John Holmes stated that it is always nice to have incident command, such as the NIMS Incident Command System, but a process is only good if people are comfortable using it. The way that people become comfortable using it is through training and exercises and by establishing the relationships one needs to use it. In Boston, New York City, and other major cities post-September 11, 2001 (9/11), there has been an intensive amount of coordination, cooperation, and attempts to get to know people through various government agencies. It is always helpful to have a structure or an entity that forces people to get together, such as maritime and air security, because once they get together, half of the problem is addressed.

Another workshop participant asked, what has been done to improve the response capabilities in Mumbai, or perhaps more generally in India, should such an attack occur again, and how much would that matter? In other words, no matter how much training one has, the reality is just so chaotic that only with incredibly good luck and good fortune could one hope to do much better than has been done in the past.

Kumar reiterated that after the incident in Mumbai, a new force called the National Investigation Agency was established. All terrorist attacks are generally in their mandate. As far as the investigation goes, and as far as the issue goes with regard to preparedness, India has one elite force called the National Security Guard. They will perhaps have a smaller contingent in Mumbai in addition to New Delhi, because earlier they had to be airlifted from Delhi to Mumbai, which took a great deal of time, and this drew adverse criticism. Also, a new agency is being created in Madras so that all eight states near Maidu Madrassa will be covered.

Thus far, forensics has not received a great deal of emphasis, but after the plethora of incidents in India, Kumar has personally seen that forensic interface increased extensively.

FORENSIC CAPABILITIES DURING THE RESPONSE PHASES, ATTRIBUTION AND PERPETRATOR PROSECUTION

The Development of Forensics Capabilities in India

Rajiv Pratap Sharma began his presentation with the etiology of forensics itself. *Criminalistics* is a word that is very often used by forensic scientists but not often used by others. It is a German word that basically refers to the use of scientific methods in the criminal investigation system, and it has been adopted into the

English language. Forensic science, until the middle of the 1950s to 1960s, was used for criminal investigations in most countries. People believed that forensic science is to provide assistance to criminal investigators, and therefore it is synonymous with forensic sciences. However, this is not true. Over time, forensic scientists gradually incorporated other areas into the domain of forensics. Sharma shared his experience at a conference about 3 years ago in Brazil. One of the scientists was talking about bringing gemology to forensics because there are odd cases that have been aided by the ability to exam a gem's size, structure, and reflection patterns. Gradually, these techniques were added to forensic sciences; they had moved from the general to the specific application. Modern scientists have divided forensics into the subcategories of pathology, nursing, investigation of traumatic death, toxicology, anthropology, taxonomy, fossilization issues, entomology, digital photo imaging, blood and bloodstain patterns, biological fluids, DNA, microanalysis, and fingerprinting. Many of these areas of forensics do exist in India, but unfortunately their growth has not been parallel to the use of forensic science in criminal investigations. That growth has been on a case-by-base basis.

References to forensics in India date back in some form to ancient literature, but in the last two to three decades, the forensic fraternity has become mature and gained importance in the country. Forensics has become more visible, and to some extent, private contributions have joined the forensics network. Currently, the government is in the process of setting accountability standards and standard operating procedures. About two to three decades ago, most of the laboratories of forensic science in India were working either under the jurisdiction of the state government or under the central government of India. There were few standard procedures to be followed, and there was not much independent evaluation of those ethics and procedures that were followed. Gradually, however, we have moved forward, and now there are checks and balances, which has improved accountability when dealing with various forensics issues.

India's first laboratory for criminal investigations was the Chemical Examiner's Laboratory, founded in 1849. Subsequently, the Anthropometric Bureau was opened in 1878, and in addition to these examples, there is a long list of labs established in the preindependence era. In 1971, the National Institute of Criminology and Forensic Science was established as an academic institution in New Delhi, which is under the jurisdiction of the Ministry of Home Affairs. The Bureau of Police Research and Development was then opened. This organization also developed a forensic science division. A Scientific Advisory Committee came into existence in the cabinet in 1999. In addition, other facilities were added for DNA typing, fingerprinting, and so forth, at our Central Forensic Science Laboratory (CFSL) in Calcutta. Further, forensic capabilities in India have gradually developed, and over the next 100 years these capabilities will be strengthened. However, despite the rapid spread of forensic services, it has been difficult to provide adequate services to meet the demand. India has a large population, as well as a large number of criminal cases. The ratio of civil to criminal disputes is about 70:30, so there are numerous criminal cases that require sup-

port and the services of forensic laboratories and forensic sciences, but unfortunately the breadth of expertise is insufficient.

The four pillars of Indian forensic science activity are located in Hyderabad, which is centrally located in India, bordered by Calcutta, Chandigarh, and New Delhi. The CFSL in Calcutta is one of India's premier institutions, established in 1957, and in addition, 25 states have regional laboratories that provide services primarily to state police organizations. There are certain central bodies, for example, the Central Bureau of Investigation, that assist and support the state police. However, although all of the services of the central laboratories are available to state police organizations, they are rarely used because state labs were used more often.

Two years ago, India had 30 million cases adjudicated by different courts across the country. A lack of forensic capabilities often delays the administration of justice because the evidentiary process of trials is long in India. Approximately 68 to 70 percent of the 30 million cases constitute criminal offenses, and though there is no data on the percentage of those criminal cases requiring forensic science, there is a lot of literature indicating that about 20 to 25 percent of all cases require the expertise of a forensic scientist. If that is the case, one or two laboratories in each of India's 25 states, together with four central forensic laboratories, are insufficient to provide the essential forensic science capabilities to deal with these criminal cases alone.

Accountability measures for forensic science in India did not develop quickly, and standard procedures were only recently implemented. Forensic scientists have to work in very challenging circumstances. They are expected to be unaffected by circumstances and to have professional thinking, professional growth, and professional expertise. Further, there is a strict division between government and private laboratories. Access to forensic laboratories is primarily only available to those with government support and those who aid investigations; private investigators do not have access to government laboratories. The labs together have 90 handwriting experts, 90 fingerprint experts, and several fingerprint assistants; there are only 9 lie detector experts, 8 failure analysis experts, and 25 DNA experts, who are microbiologists. There are 300 medical legal experts, although this does not include government medical doctors who conduct autopsies. These are the specialists in the field of forensic medicine. India has another 3,000 forensic scientists and other specialties. This is the total number of people who must assist the entire infrastructure that caters to the needs of about 30 million cases of different types that are pending different courts. On average, India adds about 207 million cases per year. The gestation period in deciding cases too often lengthens to almost 9 to 10 years. Sharma said the largest problem in the adjudication of cases is that there will be an increasing demand for forensic experts, and if India does not have enough experts, those from other countries are going to fill that vacuum. There are a few experts from Singapore and the United Kingdom who come and depose in important cases already.

Forensic science capabilities in India are largely in the public-sector domain (98 percent), 2 percent of the capabilities are in the private sector. The reason that private-sector science laboratories in the field of forensics sciences are relatively few is the lack of acceptance of their results. Experts from private labs have received little acceptance although Section 45 of the Indian Evidence Act grants them the same status as that granted to any other witness whether he or she comes from a private laboratory or from a government-sponsored lab. Because private labs have not been widely accepted, the demand for their services is insufficient to support them on a commercial basis. That is why most private industries have not grown in India, but they are slowly gaining a foothold.

Polygraph tests are widely accepted around the world, and even in a country like New Zealand, which has a very small population, there are about 30 to 40 laboratories working on these tests. Despite the questioned evidentiary value of the tests, the trend in using them is growing. There are currently seven centers in Indian that are aided and supported by the government of India that provide these tests and two polygraph laboratories are available in the private sector.

Forensic capabilities can only be developed through training linked to qualifications because the mere imparting of training does not provide expert witness status to most scientists in India. There are continuing education programs being given in some countries, but India does not have that culture. There is service training at the time of the hiring of an employee, but India has to find a way to have continuing education programs that agree with the standards of training and should be linked to partners around the world. Professional exchange opportunities, mutual professional recognition, and formal networks of mutual assistance, reviews and recognition, and accreditation are needed if India is to keep pace with the growing forensic science capabilities of the other countries.

Sharma concluded by saying that before India adopts new forensics techniques, one should be conservative and examine whether the liberties of any individual, including the accused or the suspect are being violated. Standards have to be linked to proper usage, verification, and standardization of these techniques; only if they are followed will forensic science be given respect in India. Forensic science needs to change soon or it may become irrelevant or redundant.

Overview of Forensics and Capability Needs in the United States

Romero stated that he would look back in history and compare an investigation that took place 20 years ago to the Boston Marathon bombing and examine developments over 20 years, as well as suggest where forensic science may be going. The World Trade Center (WTC) was bombed in 1993 in a coordinated terrorist attack during which 6 people were killed and 1,000 people were in-

jured.[5] A large truck was parked in an underground parking garage at the WTC, where it exploded. Fire and police were the first to respond, and they had to stabilize the scene, save lives, and look for secondary devices. In 1993, there had been few terrorist attacks on U.S. soil and there was certainly less preparation for such events than there is today. The Port Authority, which has jurisdiction over the WTC, responded right away and deemed the location unsafe, and it was even too unsafe to do any forensic collection at the time. Therefore, the first step was to put shoring in place to keep the building from falling down. The intent of the terrorists was to cause one of the towers to crash into the other as eventually happened on 9/11. They were almost successful; the building was unstable, and there was a large concern that even a hefty wind could have toppled one tower over and brought it down into the other tower.

The first step was investigating what type of device caused the explosion. This indicated the magnitude of the explosive, and it was important to know the magnitude of the explosive as a means of determining how it got there. Was it in a backpack, was it in a box, was it in a large vehicle? Obviously a crater of this size was caused by a vehicle-borne bomb. It was concluded that the device was 1,500 pounds of urea nitrate.[6]

FBI investigators had to sift through tons and tons of rubble very meticulously. Another complicating factor was that a sewage pipe had broken and all of the sewage from the building came down through that section of the garage, so the hole was filled with human sewage as well as debris from the device. It was not a very easy or pleasant place to work.

The big breakthrough in this case was finding the vehicle identification number. A piece of the axle was found and sitting next to it was the left rear frame grill. Once the frame grill was recovered, it was very easy to understand where ground zero was and where the device was actually detonated because of how the debris emanated from the blast site. It was quickly determined which vehicle was carrying the explosive device because the grill bore the vehicle ID number. Once the vehicle was identified, the investigation could turn to determining who owned the vehicle, where it came from, and how it got to where it was in the garage. It was determined that the vehicle was a Ryder rental truck. A vehicle of the same make and model was then obtained by the FBI so that Romero and his colleagues could reenact the detonation. What usually happens

[5]Romero gave special thanks to Dave Williams, who was the FBI agent who was in charge of this investigation. Romero and Williams worked very closely together as part of the investigation, and Williams provided photographs to Romero for his presentations.

[6]Romero recounted that he answered numerous questions from reporters and conspiracy theorists that saw glass on the "wrong side" of the explosion (glass flying into the explosion itself). However, depending on the geometry of any explosion, blast waves can come through and push all the air away, causing a vacuum that contracts, and if it happens quickly enough, the glass that is pushed in is then sucked out and falls on the side that is toward the device as opposed to away from the device. This is very geometry dependent, and device dependent so it is difficult to predict where the debris will go before a detonation.

in these cases is that law enforcement will put together a scenario of what occurred at the crime scene, based on collection of forensic evidence, and then they complete the investigation and, hopefully, make an arrest. Before they prosecute, they want to make sure that their theory will produce data that matches the crime scene, so the crime is reenacted in some fashion, and similar data is collected. In this case, the reenactment showed that 1,500 pounds of urea nitrate would do the type of damage to the vehicle that was found at the scene of the crime.

Ramzi Yousef was the person ultimately found responsible for the 1993 WTC bombing, but one of his colleagues rented the Ryder truck, and a few days after the detonation he returned to the rental facility to claim his deposit on the vehicle.[7] Fortunately, the FBI had already determined where the vehicle had come from and had surveillance at that location and immediately arrested the suspect. He was not the main perpetrator but was part of the team that developed the scheme. Based on the apprehension of one of the team members, they knew the location of the terrorist cell. They went to that apartment complex and talked to people in and around it and obtained several helpful eyewitness testimonies about relevant activity. They then started tracing the activity of the people that lived there and found that a number of chemical purchases were made through the company that Yousef worked for by using the company letterhead to purchase the chemicals and take them home and use them in a bomb factory. Based on eye-witness testimony, the FBI went in and served a search warrant on the location where the suspects lived, and they indeed found a bomb-making factory. Romero and his colleagues use a replica of the bomb-making factory in training programs for responders. He recalled that the responders asked many questions after the training, and when Romero inquired why, they responded: My life depends upon it. It is very important to have programs where responders learn that when they go out into the field, they can recognize a bomb factory and apprehend the perpetrator before a bomb is detonated.[8]

Urea nitrate was found in the bomb factory in the 1993 WTC case, and it was easy to identify. The only problem was that this event took place in February, and there is a lot of snow and ice in New York City in the winter. The city

[7]Yousef, who was the main leader of this terrorist act, was captured in a different country approximately 2 years after the conviction and is now in prison for life in the United States.

[8]Several firefighters went through the program, and they were given some inspections in New Jersey and they came across an apartment that was very untidy, was not well kept, and had several jugs on the floor. The police commander did not think there was a concern. They moved on to the next part of the inspection, and the firefighter who attended the class had noticed a component of urea nitrate. The FBI was called in, and they uncovered maps in the apartment of the New York—New Jersey tunnel system and with specific locations marked. If the bombs were placed at the locations indicated on the maps, they would have caused tunnels to collapse and fill with water. These people were taken into custody, but one of the concerns is that it is not illegal to own fertilizer, or ammonium nitrate, and these are common chemicals.

uses natural ice melt on the roads, which contains urea. As part of the initial response to this event, quite a lot of workers and firefighters spread these urea pellets throughout the garage and surrounding areas to melt the ice so that they would have easier access, but that contaminated the entire crime scene, as did the sewage. Unfortunately, while determining the explosive helps the investigation, it does not solve the crime. It is hard to use this as evidence in a court of law. This became important in the case because the data was called into question. The FBI crime map came under investigation when an agent questioned the forensic capabilities of the FBI lab. One of the lessons learned is that having a qualified, reputable, certified lab is paramount. One can collect great data, but if the lab is not certified, the evidence is not going to be credible in a court case.

Fastforward to 20 years later to the day of the Boston Marathon bombing. Romero recounted that there was a very interesting interview with the Boston police asking them what really helped them solve the crime. They said there were five things that were important for their forensic investigation: (1) They used robots extensively when they were investigating the crime scene because they did not know at the time whether there were other secondary devices, (2) The surveillance cameras provided key images leading to the big break, (3) They would not have solved the crime without the cooperation of the public, (4) In the ensuing chase and capture of the suspects, armored vehicles were important because the suspects were throwing grenades and had other pipe bombs and pressure-cooker bombs, (5) The thermal infrared cameras were important because once they knew there was someone in a resident's boat, they surrounded it and confirmed he was there before the final gunfight and apprehension of the suspect. They waited until it got dark and then used flash-bang grenades, which cause a lot of disruptions and disorientation. They are very loud with a lot of flashing light, and the suspect was not very sure where the attack was coming from, which was important according to the Boston police.

Romero's conclusions, based on these two cases, is that chemical analysis of explosives helps in an investigation, but not really in a trial. If a jury of people that has to make decisions about whether someone is innocent or guilty, whether he or she has used ammonium nitrate or urea nitrate or TNT, this evidence is not likely to influence their decision. Next, the primary difference between the World Trade Center bombing of 1993 and today is that there is surveillance data everywhere to be used. Media plays a significant role in these cases because they broadcast 24 hours a day, and every move made as an investigator is going to be on TV. In the Boston case, the media was used to the advantage of the investigation. In Boston, the police released information because it was their method of making sure that they controlled the situation rather than the media controlling all the information. Finally, as in both the World Trade Center bombing and the Boston bombing, there was no substitute for hard work or training and making people aware of how they can protect themselves and others.

Romero closed with his philosophy: What we really have to do is educate. If one is trained to respond to a known threat, response will be immediate, without thinking. Unfortunately, terrorists are always changing their tactics, so citi-

zens need to be educated to make critical decisions under tremendous stress. As they collect information they can make the right decision, and that is what education is about, as opposed to training.

DISCUSSION

In answer to a question about separate forensics labs in India, Sharma replied that the independence of the organization or independence of the department does not alter the scientific capabilities of the labs. There have been efforts in India to declare forensic science laboratories separate organizations and in Tamil Nadu, this has already been done. However, in some of the states, the labs work under the overall umbrella of the state government, in particular the police department. This has most likely been done to have a more harmonious approach to dealing with crime investigations, because if the labs work in isolation, team work declines. Currently in India, there are many states, such as Maharashtra and Andhra, that have already entrusted some of their work to private labs. There is one lab called Truth Labs, and in Maharashtra, one lab called Helix. Sharma feels that for an expert opinion to be sufficiently independent, it should not be under the control of the police, because the defense at a trial may raise a question about whether or not their conclusions have been manipulated by the police.

Sharma addressed the question of collaboration on developing protocols, and noted that there have been some exchange programs during which forensic scientists from India have been part of other countries' education networks, but this has not been done on a large scale. With regard to protocols, Sharma added that an experiment was carried out by the Gujarat Forensic Science Lab to establish an ethics committee to develop the protocols for brain fingerprinting. The ethics committee was headed by a sitting High Court judge.

A third question was directed to Sharma. There is a hybrid approach to forensic science used routinely elsewhere, but not in India: in some cases a government body does some of the work or outsources it on a large scale. This approach may raise the issue of credibility. Further, if people from private forensic labs are called upon to testify as expert witnesses, they may not agree or may not be available for lengthy trials, whereas government bodies have to provide all requested assistance to the courts, so the government expert witnesses may be more duty bound to act on summons, warrants, and mandates of the court. Further, those from private laboratories may require fees. Sharma replied that there may be ways to improve coordination with private labs, but only 2 percent of forensics capabilities are currently in the private sector. Developing a mechanism for greater inclusion may be much more expensive than the utility of the mechanism. However, with the latest developments in technology, there will be many companies that would like to jump into this field.

A workshop participant asked about how to build cadres of forensic scientists. Sharma answered that currently there are only 15 universities that offer forensic courses in university forensics departments, which are only one of the

many segments of an entire university. However, the lead has been taken again by Gujarat, where the first forensics university has been created. That university, Gujarat Forensic Sciences University, is the only university in India that caters to forensics needs. The placement of students who graduate from that university presently is about 100 percent. This initiative should also be emulated by other states.

Unfortunately, Sharma said candidly, if one goes through the various courses being offered by the National Institute of Criminology and Forensic Science, about 30 percent of the courses are on human rights, and these capabilities are often used in a distorted form. Currently this ratio indicates that streamlining issues is definitely required, and this holds true not only for India. This is a challenge all over the world. India does not have a single forensic entomologist employed by any government organization. So the supply and demand for developing capabilities is a large issue.

Appendix A

India-U.S. Workshop on Science and Technology for Countering Terrorism

A National Institute for Advanced Studies - National Academy of Sciences Joint Workshop

Final Agenda

FEBRUARY 3, 2014

9:30 – 9:45	**Welcome and Introductions** – V.S. Ramamurthy, *Chair*, NIAS Workshop Planning Committee – Raymond Jeanloz, *Chair*, NAS Committee on International Security and Arms Control – Norman Augustine, *Chair*, NAS Workshop Planning Committee
9:45 – 10:15	**Keynote Address: The Realities of Terrorism in India** – Nehchal Sandhu, Deputy National Security Advisor
10:15 – 11:00	**Discussion** – Led by V.S. Ramamurthy
11:00 – 11:20	**Coffee Break**
Session I	**Conceptual Approaches to Countering Terrorism** *Session Chair: R. Narasimha*
11:20 – 11:40	**Systems Approaches to Countering Terrorism** – Norman Augustine
11:40 – 12:00	**Indian Response Regarding a Systems Approach to Countering Terrorism** – Nehchal Sandhu
12:00 – 12:45	**Discussion**
12:45 – 1:45	**Lunch**

Session II	**Security at Chemical Facilities** *Session Chair: John Holmes*
1:45 – 2:05	**Securing Chemical Facilities: Recent American Experiences and Lessons Learned** – Nancy Jackson
2:05 – 2:25	**Preventing Chemical Incidents – Accidental or Intentional – Current Issues and Possible Solutions** – B. Karthikeyan
2:25 – 3:15	**Discussion**
3:15 – 3:30	**Coffee Break**
Session III	**Agricultural and Food Security** *Session Chair: A. K. Sinha*
3:30 – 3:50	**Recent Indian and American Experiences in Cooperating on Food Security** – Vedpal Yadav
3:50 – 4:10	**Securing Plants, Animals, and Crops in India** – Abraham Verghese
4:10 – 5:00	**Discussion**
5:00 – 5:30	**Coffee Break**
Session IV	**Technical Aspects of Civilian Nuclear Material Security** *Session Chair: R. B. Grover*
5:30 – 5:45	**Introductory Remarks** – V. S. Ramamurthy
5:45 – 6:00	**Release of Recent Report: *Summary of India-U.S. Workshop on Technical Aspects of Nuclear Material Security*** – R. B. Grover
6:00 – 6:30	**Overview of *Summary of India-U.S. Workshop on Technical Aspects of Nuclear Material Security*** – L. V. Krishnan
6:30 – 6:45	**Potential Areas of Cooperation Arising from the Nuclear Material Security Workshop** – Raymond Jeanloz
6:45 – 7:00	**Discussion**
7:00	**Adjourn**

FEBRUARY 4, 2014

Session V	**Global Health Security and Strengthening Public Health Infrastructures** *Session Chair: Norman Augustine*
9:30 – 9:50	**The Anthrax Letters: Lessons for Leaders** – David Franz
9:50 – 10:10	**Global Health Security in India: India's Experience with H1N1** – J. K. Bansal
10:10 – 11:00	**Discussion**
11:00 – 11:15	**Coffee Break**
Session VI	**Emergency Management and Response: All Hazards Approach** *Session Chair: Nancy Jo Nichols*
11:15 – 11:35	**Indian Experience during the Recent Himalayan Tsunami** – Vinay Kejla
11:35 – 11:55	**American Experiences during Hurricane Katrina and Superstorm Sandy** – Karl Kim
11:55 – 12:45	**Discussion**
12:45 – 1:30	**Lunch**
Session VII	**Protecting Critical Infrastructure** *Session Chair: Nancy Jackson*
1:30 – 1:50	**Enhancing the Security of India's Critical Infrastructure: Aviation Security** – B. K. Maurya
1:50 – 2:10	**Recent Experience with Averted Power Failure in Silicon Valley** – Michael O'Brien
2:10 – 2:30	**A Practical Approach to Infrastructure Protection: Lessons from the Field** – John Holmes
2:30 – 3:15	**Discussion**
3:15 – 3:30	**Coffee Break**

Session VIII	**Cybersecurity in its Complexity** *Session Chair: N. Balakrishnan*
3:30 – 3:50	**Understanding Cybersecurity and Related Challenges** – Srinivas Mukkamala
3:50 – 4:10	**Cybersecurity Challenges in India** – B. J. Srinath
4:10 – 5:15	**Discussion**
5:15 – 5:30	**Coffee Break**
5:45 – 6:30	**Screening of *Terror in Mumbai***
6:30 – 8:00	**Dinner at NIAS**

FEBRUARY 5, 2014

Session IX	**Case Studies from India and the United States** *Session Chair: Byron Gardner*
9:00 – 9:30	**Experiences of Science and Technology to Counter Terrorism: Incidents in India** – Keshav Kumar
9:30 – 10:30	**Screening of *Manhunt. Boston Bombers. Technology's Role in Catching the Marathon Bombing Suspects***
11:05 – 11:25	**The Boston Marathon Attacks** – Van Romero
11:25 – 11:50	**Discussion**
Session X	**The Challenges of Conventional Terrorism** *Session Chair: S. Gopal*
11:50 – 12:10	**Technologies for Countering Terrorism** – K. Sekhar
12:10 – 12:30	**Developing Comprehensive Training for Future Explosives Experts** – Byron Gardner
12:30 – 1:00	**Discussion**
1:00 – 1:45	**Lunch**

Session XI	**Forensics Capabilities during Response Phases, Attribution and Perpetrator Prosecution** *Session Chair: Keshav Kumar*
1:45 – 2:05	**The Development of Forensics Capabilities in India** – R. P. Sharma
2:05 – 2:25	**Overview of Forensics and Capability Needs in the United States** – Van Romero
2:25 – 2:45	**Discussion**
2:45 – 3:00	**Coffee Break**
Session XII	**General Discussion and Suggested Future Actions** *Session Co-Chair: Stephen P. Cohen* *Session Co-Chair: Gen. Sundaram*
3:00 – 3:30	**Additional Comments and Suggestion**
3:30 – 3:45	**Closing Remarks** – V.S. Ramamurthy – Norman Augustine – Lalitha Sundaresan
3:45	**Adjourn**

Appendix B

Statement of Task

An ad hoc organizing committee under the auspices of the National Academy of Sciences standing Committee on International Security and Arms Control will work with partner organizations in India to convene an Indian-U.S. workshop on science and technology for countering terrorism. The organizing committee and its counterpart in India will develop the workshop agenda, select and invite speakers and discussants, and moderate the discussions. The agenda will include topics to address biological threats (health and agriculture); protection of nuclear facilities; security (physical and cyber) for chemicals, chemical facilities, and other critical infrastructure; and monitoring, surveillance, and emergency response. It will also include topics to identify and examine promising areas for further Indian-U.S. cooperation on science and technology for countering terrorism.

Appendix C

Biographical Sketches of Workshop Speakers and Session Moderators

Norman R. Augustine (National Academy of Sciences [NAS], National Academy of Engineering [NAE]), *chair*, is the retired chairman and chief executive officer of the Lockheed Martin Corporation and a former under secretary of the army. Augustine served as a member of the President's Council of Advisors on Science and Technology and the Department of Homeland Security's (DHS) Advisory Council. He chaired the NAS committee that authored the report *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future*. Among Augustine's many honors are the National Medal of Technology and the Department of Defense's (DOD) highest civilian award, the Distinguished Service Medal, given to him five times. He was awarded the 2005 American Association for the Advancement of Science (AAAS) Philip Hauge Abelson Prize and the 2006 Public Welfare Medal from NAS.

Augustine also served as chairman and principal officer of the American Red Cross for 9 years and as chairman of the NAE, the Association of the United States Army, the Aerospace Industries Association, and the Defense Science Board. He is a former president of the American Institute of Aeronautics and Astronautics and the Boy Scouts of America. He is a current or former member of the Board of Directors of ConocoPhillips, Black and Decker, Procter & Gamble, and Lockheed Martin, and is a member of the board of trustees of Colonial Williamsburg, a trustee emeritus of Johns Hopkins, and a former member of the board of trustees of Princeton University and Massachusetts Institute of Technology (MIT). He holds 18 honorary degrees. Augustine graduated magna cum laude from Princeton University, where he earned bachelor's and master's degrees in engineering. He is the author of *Augustine's Travels*, *The Defense Revolution*, and *Augustine's Laws*.

N. Balakrishnan is currently the associate director of the Indian Institute of Science and a professor at the Department of Aerospace Engineering and at the Supercomputer Education and Research Centre. His areas of research where he has several international publications include numerical electromagnetics, high performance computing and networks, polarimetric radars, aerospace electronic

systems, information security, complex social networks, and digital library. He is a fellow of the World Academy of Sciences, Indian National Science Academy, Indian Academy of Sciences, Indian National Academy of Engineering (INAE), National Academy of Sciences, and Institution of Electronics and Telecommunication Engineers. He has received many awards, including the Padmashree by the President of India, Professor S.N. Mitra Memorial Award 2013 from INAE, and J.C. Bose National Fellowship 2007. He has served as a member of the National Security Advisory Board for many years. He was on the Board of Governors of IIT Chennai and Delhi, Bharat Electronics Limited and the Telecom Regulatory Authority of India. Currently he is on the Data Security Council of India, Central Bank of India, Bharat Sanchar Nigam Limited, CDOT-Alcatel Research Center at Chennai, Center for Development of Advanced Computing, Indian Statistical Institute of Kolkata, IIT Kharagpur, and the Joint Advisory Board of Carnegie Mellow University at Qatar. He is an honorary professor at the Jawaharlal Nehru Centre for Advanced Scientific Research.

J. K. Bansal is the Honorable Member of the National Disaster Management Authority (NDMA), government of India, having the status of Union Minister of State. Previously, he served in the Army Medical Corps and the Defense Research & Development Organization (DRDO). He is a medical doctor with a specialization in thyroid diseases. He established the Chemical, Biological, Radiological, Nuclear (CBRN) mitigation division and the Chemical, Biological, Radiological, Nuclear Training Center at the Defense Research and Development Establishment (DRDE) at Gwaloir. He is the pioneer of the Radiation Disaster Medical Management Center, Institute of Nuclear Medicine and Allied Sciences, Delhi. He underwent extensive professional training in CBRN mitigation and environmental help in Australia, Canada, Holland, Japan, Russia, and Sweden. He participated in a task force meeting of Organisation for the Prohibition of Chemical Weapons (OPCW), The Hague, Holland for evaluation of protection and treatment of chemical injuries in 1995. He attended the International Basic Course on Chemical Weapon Assistance and Protection at Rescue Services College, Revinge, Sweden, in 2002, and at Training Centre Krusevac, Serbia, in 2009.

He has wide experience with CBRN protection, detection, decontamination and medical management. He visited the Joint Institute for Nuclear Research in Dubna, Moscow, where he gained practical experience and became acquainted with and updated about nuclear disaster management. He published large numbers of papers on chemical terrorism disaster management. He presented the "Indian Perspective on Bioterrorism Prevention and Response" during the Interpol Workshop on Bioterrorism Prevention in 2007. He delivered the keynote address at the inaugural session of the OPCW Conference on International Cooperation and Chemical Safety and Security held at The Hague, Netherlands, in 2011. He made very significant contributions in a high-level roundtable meeting of international experts on "Enhancing Global Security: Multi-Sectoral Ap-

proaches to Mitigating Infectious Disease Threats," held on June 11, 2013, hosted by Chatham House London. He made major contributions in prevention and management of the swine flu pandemic in 2009. He was deeply involved in the management of the chlorine gas leak at Mumbai port during 2010. He successfully managed the radiation emergency, including medical treatment, during the Mayapuri radiation incident in 2010. He contributed significantly during natural disaster such as tsunamis, the Gujarat earthquake and the Orissa super cyclone. For his outstanding contribution and distinguished services, the president of India decorated him with the Vishist Sewa Medal. He was awarded the Chiktisa Ratan by Delhi Medical Association for his outstanding contribution in training medical doctors for CBRN disaster casualties management.

Stephen Philip Cohen has been senior fellow in foreign policy studies at the Brookings Institution since 1998. In 2004, he was named as one of the 500 most influential people in the field of foreign policy by the World Affairs Councils of America. Cohen was a faculty member at the University of Illinois from 1965 to 1998. From 1992 to 1993 he was scholar-in-residence at the Ford Foundation, New Delhi, and from 1985 to 1987, a member of the Policy Planning Staff of the U.S. Department of State, where he dealt with South Asia. He has taught at Andhra University (India) and Keio University (Tokyo), and Georgetown University, and now teaches in the South Asian program of Johns Hopkins School of Advanced International Studies. Cohen has served on numerous study groups examining Asia sponsored by the Asia Society, the Council on Foreign Relations, the Asia Foundation, and the National Bureau of Asian Research. He is a trustee of the Public Education Center. Cohen was the co-founder and chair of the workshop on Security, Technology and Arms Control for younger South Asian and Chinese strategists, held for the past 10 years in Pakistan, India, Sri Lanka and China, and was a founding member of the Research Committee of the South Asian strategic organization the Regional Centre for Security Studies, Colombo. Cohen has written, co-authored, or edited 10 books. Cohen received B.A. and M.A. degrees in political science from the University of Chicago, and a Ph.D. in political science from the University of Wisconsin. He has conducted research in Britain, China, Japan, India, Pakistan, and the former Soviet Union. He received grants from several major foundations and serves as a consultant to numerous government agencies.

David R. Franz served in the U.S. Army Medical Research and Materiel Command for 23 of 27 years on active duty and retired as colonel. He served as commander of the U.S. Army Medical Research Institute of Infectious Diseases and as deputy commander of the Medical Research and Materiel Command. Prior to joining the Command, he served as group veterinarian for the 10th Special Forces Group (Airborne). Franz was the chief inspector on three United Nations Special Commission biological warfare inspection missions to Iraq and served as technical advisor on long-term monitoring. He also served as a member of the first two U.S.-U.K. teams that visited Russia in support of the Trilat-

eral Joint Statement on Biological Weapons and as a member of the Trilateral Experts' Committee for biological weapons negotiations. Franz was technical editor for the *Textbook of Military Medicine on Medical Aspects of Chemical and Biological Warfare,* released in 1997. Current standing committee appointments include NAS Committee on International Security and Arms Control (CISAC), the National Research Council (NRC) Board on Life Sciences, the Department of Health and Human Services National Science Advisory Board for Biosecurity, and the Senior Technical Advisory Committee of the National Biodefense Countermeasures Analysis Center. He serves as a senior mentor to the Program for Emerging Leaders at the National Defense University. He also serves on the Board of Integrated Nano-Technologies, LLC. Franz holds an adjunct appointment as professor for the Department of Diagnostic Medicine and Pathobiology at the College of Veterinary Medicine, Kansas State University. The current focus of his activities relates to the role of international engagement in the life sciences as a component of global biosecurity policy. Franz holds a D.V.M. from Kansas State University and a Ph.D. in physiology from Baylor College of Medicine.

Byron Gardner leads the critical infrastructure protection program at Lawrence Livermore National Laboratory (LLNL). This program concentrates on the protection of globally strategic energy facilities. Gardner's areas of knowledge and expertise include: vulnerability assessments of energy and nuclear facilities; high-security system design; familiarity with security system technologies, regulations, and operations; management of major security system implementation projects; insider threat analysis and mitigation; security system performance testing; and security systems training and regulatory development. Gardner has worked on high-security systems for more than 39 years. His educational training is in systems management with a bachelor's degree from the University of New Mexico and graduate studies in law enforcement and counterterrorism, as well as specialized training in multiple safeguards and security disciplines. Gardner's project teams have received numerous commendations from domestic and foreign customers for work conducted on some of the world's most important nuclear and critical facilities. Gardner managed more than $400 million in upgrades to Russian nuclear weapon bases. Gardner has worked in 24 countries and has worked on security projects for the DOD, Department of Energy (DOE), DHS, and National Regulatory Commission in 28 U.S. states.

S. Gopal worked with the government of India for more than three and a half decades, during which he had wide experience in the analysis of national and international security and strategic affairs. After retirement, he was instrumental, along with other colleagues, in establishing the Institute of Contemporary Studies in Bangalore. The institute started a quarterly journal called *Contemporary Analyst*, in which Gopal has been a regular contributor. One of his more important papers was on the Comprehensive Test Ban Treaty (CTBT), entitled, "India and the CTBT." He is a member of the Asia Centre in Bangalore, where

he presented a paper assessing Pakistan's security scenarios. In a seminar on Naxalism organized by the Observer Research Foundation in Chennai, he presented a paper entitled, "The Naxalite Movement: Impact of External Networking." In a seminar in Sri Lanka, recently organized by the Indian Centre for South Asian Studies and the Centre for Asia Studies, Gopal presented a paper entitled, "The Role of the Janatka Vimukti Peramuna in Sri Lankan Politics," with particular reference to the ethnic question. Gopal also has wide experience in technical and imagery intelligence analysis.

Ravi B. Grover graduated in mechanical engineering from Delhi College of Engineering in 1970 and joined the Bhabha Atomic Research Centre (BARC) Training School to study nuclear engineering. He worked as a nuclear engineer for 25 years and specialized in thermal hydraulics. Simultaneously, he obtained a Ph.D. from the Indian Institute of Science (IIS), Bangalore in 1982. Presently, he is working as a principal advisor at the Department of Atomic Energy (DAE) and is a member of the Atomic Energy Commission. He is concurrently working as director of the Homi Bhabha National Institute, and is responsible for running the university. As principal adviser, he deals with issues related to the nuclear power policy of India, including the evolution of the nuclear legislative framework, energy studies, and international collaborations. Grover was a member of the team of officials involved in negotiations that led to the opening up of international civil nuclear cooperation. He is also chair of the Indian delegation to the International Thermonuclear Experimental Reactor Council. He served as a member of the expert group, constituted by the director general of the International Atomic Energy Agency (IAEA), to examine multilateral approaches to the nuclear fuel cycle. Grover is an INAE fellow and president of the Indian Society of Heat and Mass Transfer. His recent awards include the INS Award in 2006 for Nuclear Reactor Technology, including nuclear safety; the Dhirubhai Ambani Oration Award in 2008; the Distinguished Alumnus Award in 2009 from the Delhi College of Engineering Alumni Association; and the Distinguished Alumnus Award in 2011 from the IIS and the IIS Alumni Association.

John Holmes is former deputy executive director of operations at the Port of Los Angeles, where he oversaw the Port Police, Port Pilots, Emergency Preparedness, Wharfinger, and Homeland Security divisions at the number one container port in the nation. Holmes held the ultimate responsibility for Port-related security and public safety issues. His divisions worked cooperatively with associated government and law enforcement agencies to uphold maritime laws, enforce safety and security regulations, and continually test and enhance emergency response and preparedness procedures to ensure the safety of the Port workforce and residents in the surrounding harbor communities. Holmes has 30 years of international management experience in a variety of positions that include chief operating officer, Fortune 500 executive, senior level Coast Guard officer, and maritime security specialist. He most recently served as a principal and chief operating officer of the Marsec Group, a full-service security consult-

ing firm specializing in supply-chain security, technology and operations. Prior to forming the Marsec Group, Holmes was vice president and director of business development for Science Applications International Corporation, where he assisted government and commercial customers with the development of technological solutions to homeland security challenges, with an emphasis on port, border, and military solutions.

Holmes retired from the U.S. Coast Guard in 2003 following 27 years of distinguished service in a variety of posts that included commanding officer, officer in charge of marine inspection and captain of the port for the Los Angeles Long Beach port complex. As captain of the port, Holmes was at the helm on September 11, 2001, and has been credited with swift and decisive actions that ultimately led to the creation of a number of national security initiatives, including the Maritime Transportation Security Act, Area Maritime Security Committee, and National Sea Marshal Program. Earlier in his Coast Guard career, he served as deputy chief of the Coast Guard Office of Congressional Affairs in Washington, D.C. and as delegate and committee chairman at the International Maritime Organization in London. Holmes holds bachelor's degrees in English and education from Boston College, and a master's degree in business administration from Washington University's John M. Olin School of Business.

Nancy B. Jackson is manager of the International Chemical Threat Reduction Department in the Global Security Center at Sandia National Laboratories (SNL), which assists the U.S. Department of State and other federal agencies in solving problems related to international chemical security. With the Department of State, Jackson has developed the Chemical Security Engagement Program (CSP), an international program to raise awareness of chemical safety and security among chemical professionals and to enable the practice of safety and security in the research, teaching, and commerce of chemicals. CSP has worked with universities and small to medium chemical companies in Southeast Asia, South Asia, the Middle East, and North Africa. Her group is responsible for encouraging the safe and secure practice of chemicals in an effort to prevent their misuse as weapons, poisons, explosives, or environmental pollutants. This includes providing training in laboratory safety, process safety, and physical security.

Previously, Jackson was deputy director of SNL's International Security Program, where she assisted the director in fulfilling its mission to create technology-based solutions through international cooperation to reduce the threat of weapons of mass destruction (WMD) proliferation and terrorism. Prior to her positions in global security, Jackson was a principal investigator in heterogeneous catalysis with an emphasis on energy applications. Later work involved chemical imaging with a wide variety of applications from biological systems to homeland defense problems. Jackson is a national affiliate of NAS where she has served on several boards and chaired studies. She is a fellow of AAAS and

the International Union of Pure and Applied Chemistry and was recipient of the 2005 American Indian Science and Engineering Society Professional of the Year Award. In 2009, she was elected to the presidential succession of the American Chemical Society. She served as president-elect for 2010, president for 2011, and immediate past president for 2012. She is a research associate professor at the Chemical and Nuclear Engineering Department of the University of New Mexico. Jackson has a B.S. degree in chemistry from George Washington University from which she won a Distinguished Alumni Achievement Award in 2005 and has a Ph.D. in chemical engineering from the University of Texas at Austin.

Raymond Jeanloz (NAS) is professor of earth and planetary science and of astronomy at the University of California at Berkeley. He has done pioneering work in mineral physics, measurement of materials properties, and simulation of deep-Earth processes using diamond-anvil and shock-wave experiments, elucidation of the core-mantle boundary as a chemically reactive zone, and study of the role of water in mantle processes and deep earthquake generation. His research and teaching have been recognized through a MacArthur Award, the American Geophysical Union's Macelwane Award, and fellowship in the American Academy of Arts and Sciences and AAAS. He has previously served as chair of the NRC's Board on Earth Sciences and Resources. He currently serves as the chair of the NAS CISAC.

Vinay Kajla is a joint advisor at NDMA. He holds a B.Sc. in physics from Delhi University and an M. Com. in business administration from Rajasthan University. Kajla joined Central Industrial Security Force (CISF) in 1994 and has gained wide-ranging experience throughout his career. He has served at Narora Atomic Power Station, HFCL Barauni, EDP Cell of CISF HQ, National Industrial Security Academy Hyderabad, Uri and Dulhasti Hydel Power Stations in Jammu and Kashmir, and Mumbai Port Trust. He has participated in numerous disaster management courses in India and abroad. He also participated as the joint advisor for operations during the recent Uttrakhand flashfloods incident, particularly in Kedarnath and Badrinath. He participated in managing the neutralization of chlorine and other hazardous cylinders at Mumbai Port Trust in July 2010. Additionally, Kajla helped set up the Joint Operational Command Centre, which helped restore Port Traffic just 5 days after the accident of MSC Chitra with Khalijia in August 2010. He took part in various landslides operations at Assar on Jammu Kishtwar highway in Jammu and Kashmir in February 2009 and also coordinated airport operations during the Bhuj earthquake in January 2001.

B. Karthikeyan is a chemical engineer from Madras University, India, with more than 35 years of experience in the chemical industry in operations, technical services, process safety, occupational health and safety, and environmental management. He has worked in India and abroad. His extensive practical expe-

rience includes the implementation and auditing of the Process Safety Management Program, Environmental Management System as per International Organization for Standardization 14001 and Occupational Health and Safety Advisory Services 18001 systems. He is also an emergency responder for chemical plants and has undergone extensive emergency response and rescue training abroad. He has investigated numerous chemical process plant incidents using Event and Causal Factor Analysis, Man-Technology-Organization Analysis, and barrier analysis techniques and is an expert on human factors and abnormal situation management. He has worked at senior management levels with leading organizations, such as Madras Fertilizers Limited, Murugappa Group (as deputy general manager for process safety management), and internationally with National Methanol Co., Saudi Arabia (a SABIC and Celanese joint venture). He has carried out more than 400 audits of process safety, and environmental management systems in both continuous and batch processes, chaired many Hazard and Operability Analysis studies and conducted more than 350 training sessions on management systems for process safety.

Karl Kim is professor of urban and regional planning at the University of Hawaii, where he also directs the Disaster Management and Humanitarian Assistance Program and serves as the executive director of the National Disaster Preparedness Training Center (NDPTC). NDPTC is part of the national Domestic Preparedness Consortium, funded by DHS, Federal Emergency Management Agency (FEMA). He has been elected the incoming chairman of the Consortium. In addition to holding appointments in the School of Architecture and the Center for Korean Studies, Kim has previously served as the vice councilor for academic affairs (chief academic officer), overseeing tenure and promotion, program review, international programs and strategic planning for the research campus of the University of Hawaii. He has been principal investigator for research and training projects funded by international, federal, and as state and local agencies and organizations. Kim has served as editor of *Accident Analysis and Prevention*, a leading journal on transportation and industrial safety, and is author of *Learning from Disaster: Planning for Resilience* (Routledge, forthcoming). He is also editor of a special issue of the *Journal of the American Planning Association* on disaster recovery. He is author of more than 70 refereed journal articles on risk assessment, urban planning, environmental management, and disaster studies. He has been a Fulbright Scholar to Korea and to the Russian Far East. He was educated at Brown University and MIT.

L. V. Krishnan is currently adjunct faculty at the National Institute for Advanced Studies (NIAS). He joined DAE in 1958 after taking an honors degree in physics from Madras University. Later, he graduated from the Oak Ridge School of Reactor Technology in 1964. He served in the Health Physics Division at Trombay from 1959 until 1973 and then moved to the Kalpakkam Centre to set up the Safety Research Laboratory. At Trombay, he served as plant health physicist for some time. He has participated in safety evaluation of various nu-

clear installations including power reactors and reprocessing plants. At Kalpakkam, he was chairman of the Safety Evaluation Working Group and retired in 1997 as director of the Safety Research and Health Physics Group. His current interests are related to energy and the environment scene in India. He co-authored a book entitled *Atomic Energy in India – Fifty Years*, with C. V. Sundaram and T. S. Iyengar, and another book entitled *Elements of Nuclear Power* with Raja Ramanna.

Keshav Kumar is a joint director at the Central Bureau of Investigation (CBI) in Mumbai, India. He joined the Indian police service in 1986, and until recently he served in the state of Gujarat. He completed the Advance Physical Security Training Programme at the Federal Law Enforcement Training Center in Glynco, Georgia. He was selected for the U.S. International Visitor's Leadership Fellowship Program in June 2009. He has been actively associated with forensic sciences and was instrumental in establishing the Wildlife Crime Cell. In 2013, he was awarded the "Wildlife Service Award" by *Sanctuary Asia Magazine* in recognition of his contributions to wildlife forensics.

Bijaya Kumar Maurya is an Indian Police Service (IPS) officer since 1990 and he belongs to the Uttar Pradesh Cadre. He graduated with a degree in mechanical engineering with a Gold Medal from the Indian Institute of Technology, B.H.U. Varanasi. He has 23 years of experience in police service with honors. He was district police chief of eight districts in Uttar Pradesh which includes Faizabad, Bareilly, Aligarh, Agra, and Muzzaffar Nagar. He was also deputy inspector general of Azamgarh, Saharanpur, and Meerut Ranges of Uttar Pradesh. On deputation to the government of India, he headed the Intelligence Unit of Paramilitary Organization Sashastra Seema Bal and further, on promotion to the rank of inspector general, he was posted as inspector general (North-West Frontier) of Indo-Tibetan Border Police (ITBP) and inspector general (administration and training) at the Directorate General of ITBP. He worked at the United Nations for 1 year (2000-2001) as a member of the civil police in Peace Keeping Mission in Kosovo, Europe. At present, he is executive director of security, Air India Limited, the national air carrier of India. He has been selected as a member of the Security Working Group of the International Air Transport Association to be a part of the Safety, Operations, and Infrastructure team to advise on security issues affecting the airline industry. He is a recipient of the Indian Police Medal for meritorious service for 2007. He was also awarded with the Director General's Commendation Roll and Insignia in 2010 and 2012.

Srinivas Mukkamala is one of Computational Analysis and Network Enterprise Solutions' (CAaNES), LLC. owners and its chief technology and operations officer. He is a senior research scientist with the Institute for Complex Additive Systems Analysis, a statutory research division of New Mexico Tech, performing work on information technology, information assurance and protection of critical infrastructures. He is also an adjunct faculty member with the

computer science department of New Mexico Tech. He serves as a government and industry liaison and leads the New Mexico Cyber Strike Team to provide information and network security to CAaNES clients. Mukkamala has more than 80 publications in the areas of information security, digital forensics, data mining, simulation and modeling, and bioinformatics. His current research is focused on intrusion and threat analysis, risk management, vulnerability assessments, digital forensics, malware mitigation and prevention, machine learning, data mining, and information security. Mukkamala received his M.S. and Ph.D. in computer science from New Mexico Tech.

R. Narasimha, former director of NIAS, currently Department of Science and Technology (DST) Year-of-Science Professor at the Jawaharal Nehru Centre for Advance Scientific Research, helped initiate a series of dialogues with NAS CISAC on matters related to international security, with particular reference to nuclear weapons. He is an aerospace scientist, who has been widely honored for his work. He is a foreign associate of both NAS and NAE. He has served as a member of the Space Commission and of the National Advisory Board for several years.

Nancy Jo Nicholas has been a member of Los Alamos National Laboratory's (LANL) technical staff since 1990, and is the director of LANL's Nuclear Nonproliferation Program Office. From June 2006 to June 2010 she served as the LANL Nuclear Nonproliferation Division Leader responsible for 250 people who executed a significant nonproliferation mission. Prior to that she headed LANL's Nonproliferation and Security Technology Program Office where she grew nuclear safeguards programs and helped place LANL personnel in key nonproliferation positions in Washington and Vienna. She previously served as deputy group leader for the LANL's Advanced Nuclear Technology Group, helping manage an operational Cat I nuclear facility. She has served several assignments at the International Safeguards Division at DOE/National Nuclear Security Administration Headquarters and at the Rocky Flats Environmental Technology Site. Nicholas serves as vice chair of the Board of Directors and founding board member of WINS—the Vienna-based World Institute for Nuclear Security. She was elected and recently served a 2-year term as president of the Institute for Nuclear Materials Management, the premiere international professional society for nonproliferation and safeguards. She has extensive experience in both line and program leadership. Her technical field of expertise is nondestructive assay measurements. Nicholas earned a B.S. in mathematics and physics from Albright College and an M.S. in nuclear physics from George Washington University.

Michael O'Brien is responsible for managing and providing technical support in the protection of nuclear and infrastructure assets deemed critical to U.S. national security. He currently holds the LLNL position of associate program leader for the Global Security Directorate's International Nuclear Material Protec-

tion Program and has more than 30 years of domestic and international experience in the fields of vulnerability assessment, including insider analysis, and physical protection. He has participated in vulnerability assessments, insider analyses, training, regulatory development, inspections, and security upgrades of sites in the United States and world-wide. He has served on Department of Army, Department of Navy, and DOE working groups for the formulation of physical protection policy guidance and regulations and has provided similar support under the U.S. government bilateral work with the European Commission, IAEA, Russian Federation, and China. O'Brien also supports DOE's Global Critical Energy Infrastructure Protection Program activities in the international oil and electricity sectors. O'Brien holds a B.A. from the University of Maryland.

Valangiman Subramaniam Ramamurthy is a well-known Indian nuclear scientist with a broad range of contributions from basic research to science administration. Ramamurthy started his career at BARC, Mumbai, in 1963. He has made important research contributions, both experimental and theoretical, in many areas of nuclear fission and heavy ion reaction mechanisms, statistical and thermodynamic properties of nuclei, physics of atomic and molecular clusters, and low energy accelerator applications. From 1995 to 2006, Ramamurthy was fully involved in the promotion of science in India as secretary to the government of India, DST in New Delhi. He was also the chairman of the IAEA Standing Advisory Group on Nuclear Applications for nearly a decade. After retirement from government service, Ramamurthy, in addition to continuing research in nuclear physics in the Inter-University Accelerator Centre in New Delhi, has also been actively involved in human resource development in all aspects of nuclear research and applications. Ramamurthy is also a chair of the Recruitment and Assessment Board for the Council of Scientific and Industrial Research and a member of the National Security Advisory Board. In recognition of his service to the growth of S&T in India, Ramamurthy was awarded one of the top civilian awards of the country, the Padma Bhushan Award, by the government of India in 2005. Ramamurthy is presently the director of NIAS.

Van Romero is currently the vice president for research, a professor of physics and the chief officer of the Research and Economic Development Division of New Mexico Institute of Mining and Technology (New Mexico Tech). He obtained his B.S. and M.S. in physics from New Mexico Tech and his Ph.D. in physics from the State University of New York at Albany. Romero is a founding member and served as the chair of the National Domestic Preparedness Consortium (NDPC). The NDPC is a training partner for FEMA. Since its formation as a result of the Oklahoma City bombing, the NDPC has trained more than 2 million first responders from every state and territory. Romero's and New Mexico Tech's contribution to the consortium has been to develop and deliver training in the area of explosives and incendiary devises. Prior to becoming the vice president for research, Romero was the director of the Energetic Materials Research

and Testing Center at New Mexico Tech. During this time he participated in and provided oversight for all aspects of energetic materials research. This work included the experimental activity that provided the data to DHS/Transportation Security Agency for the development of the 3-1-1 rule used to allow small amounts of liquid on board airplanes. Before joining the university, Romero worked at four DOE laboratories conducting research in nuclear radiation and spent 15 years in the private sector.

Nehchal Sandhu was appointed deputy national security advisor in the Indian Prime Minister's Office on March 21, 2013. A career officer of the Indian Police Service, Sandhu put in 39½ years after his initial appointment in July 1973. During that extended tenure, the first 5 years were spent in field-level policing, involving prevention of crime, investigation, detection and prosecution in specific jurisdictions in the eastern Indian province of Bihar. Later, Sandhu served in CBI and during the last 2 years of that tenure, he headed this bureau as its director. During much of this period, his duties related to the countering of terrorism, analysis of disruptive trends, security management and technological upgradation. He served overseas in Canada as counsellor in the High Commission of India in Ottawa in the mid-1990s and is widely traveled. He was chairman of the Asia Pacific World Regional Office of the International Association of Chiefs of Police for 2 years (2011 and 2012). Sandhu is the proud recipient of the Indian Police Medal for Meritorious Service (1998), President's Police Medal for Distinguished Service (1998), and several commendations. Sandhu graduated with honors in science from St. Stephen's College, Delhi, and maintains a keen interest in technological developments.

K. Sekhar obtained his B.Tech. (Honors) in chemical engineering from IIT, Kharagpur in 1971 and M. Tech. in chemical engineering from IIT Madras in 1973. He obtained his doctorate degree from Jiwaji University, Gwalior. Sekhar joined Defence Research and Development Laboratory (DRDL) in Hyderabad in October 1973 as a senior scientific officer. He worked on liquid propulsion technology for 16 years. During this tenure, he has set up a large-thrust liquid rocket engine test facility, and tested and evaluated the propulsion stages of PRITHVI and AGNI missiles. As project executive he has set up production facilities at 10 ordnance factories for the production of propellants and explosives required for the IGMDP missile program. In his role as the director of reliability and quality assurance, at DRDL, Hyderabad, he ensured the quality and reliability of all missile systems during the development and limited series production phase. Sekhar took over as director of DRDE, Gwalior, in November 2001. During his tenure of 5½ years as director, he has brought in product orientation leading to the development of several diagnostic kits and nuclear, biological, chemical (NBC) protective equipment. This has culminated in equipping a third of the army with NBC protective devices. During his tenure, DRDE has come into the select group of labs in the world that are designated as official OPCW labs to identify trace quantities of chemical warfare agents in several

matrices. He also held additional charge as director of the Defence Materials and Stores Research and Development Establishment from November 2004 to February 2005. He was a member of the Secretary of Professor P. Rama Rao DRDO Review Committee constituted for the revamping of DRDO.

He has several publications (32), national and international patents (102 and 31, respectively), and distinguished awards. He has been the chairman of international organizations (Confidentiality Commission of the OPCW) and is a fellow and member of several professional societies. He was the chief controller of R&D (implementation) up to October 2009 and then served as chief controller of R&D, Missile Systems and Low Intensity Conflict (MS & LIC), at the corporate headquarters until May 1, 2011. Later, he took over as chief controller of R&D, LIC, and Implementation at DRDO headquarters, New Delhi. He retired from DRDO on May 31, 2012. He has been vice chancellor of Vels University, Chennai, since April 2013.

Rajiv Pratap Sharma has been an Indian police service officer since 1987, graduating with the Karnataka Cadre and was awarded Indian Police Medal for Meritorious Services on the eve of Independence Day in 2007. He is an internationally known scholar in the field of forensic sciences and legal medicine. He was the vice president of the Indo-Pacific Association of Law, Medicine and Forensic Science for two terms. He is a distinguished member in council of the International Association of Legal Medicine. In academics, Sharma has exhibited his talent by acquiring M.B.B.S. (Honors), L.L.B., and diplomate from the American Board of Examiners in Crisis Intervention and fellow from the American College of Forensic Examiners Institute in the field of crisis intervention. In his distinguished career spanning more than 26 years, he has served in various capacities as superintendent of police of many districts, inspector general of police of the Southern Range of Karnataka and presently he is holding the post of additional director general of police of the Bangalore Metropolitan Task Force. He has served in the Union of India on deputation as deputy inspector general of police, Sashastra Seema Bal. He has attended as delegate in various international conferences in different parts of the world and presented many papers on various subjects ranging from police issues to the issues pertaining to forensic sciences, law and jurisprudence. His various papers published in many law journals have been acclaimed as of high quality by legal scholars. The reformatory changes introduced as additional director general of police, Bangalore Metropolitan Task Force in the planning, execution, and detection have been widely appreciated by the residents of Bangalore and also by distinguished and eminent personalities such as Sri Santhosh Hedge, former Lokayukta of Karnataka. He was awarded the Commendation Disc and Commendation Roll of the Director General, Sashastra Seema Bal, in 2006. He has also published several books, including *Citizen and Human Rights* (1997), *Prevention of Crime* (1998), *Observation of National Disaster Reduction Day*, and *Integrated Approach to Disaster Management*, and edited the *Civil Defense Plan for Karnataka State*.

A. K. Sinha is a serving paramilitary officer from Sashastra Seema Bal and is presently working as senior research officer with NDMA. His current responsibilities include policy research, program planning, and interagency coordination for CBRN disaster management, including weapons of mass destruction and terrorism. With an M.V.Sc., he specializes in biological disaster management, including bioterrorism and biosecurity. As a core group member, he has been associated with NDMA since its inception, and has contributed to the formulation of the National Guidelines on Biological Disaster Management, Medical Preparedness and Mass Casualty Management, Management of the Dead in the Aftermath of Disaster, NDMA-World Health Organization Action Plan on Pandemic Preparedness Beyond Health, and Plan to Counter the Threats to the Municipal Water Supply and Water Reservoirs. In addition to NDMA, he actively contributes to biorisk management capacity-building programs of DRDO, the Indian Council of Agriculture Research, the National Institute of Disaster Management, and the State Administrative Training Institutes. Sinha has expertise in biosecurity and bioterrorism. As a technical expert from NDMA, he has been associated with the Disarmament and International Security Affairs Division of the Ministry of External Affairs (MEA), and was also a member of the Indian delegation to the UN Biological Toxin and Weapons Convention (BTWC) in Geneva in 2008, and the Biodefense Congress in Kuala Lumpur in 2011, the BTWC Review Conference in Geneva in 2011, and the Association of Southeast Asian Nations Regional Forum Workshop on Biorisk Management in Manila in 2012. During his association with MEA and international exchanges, he contributed significantly to strengthening India's foreign policy obligations on global biorisk management. Currently, Sinha is coordinating NDMA's Biological Disaster Management Program and capacity-building program on CBRN Prevention, Preparedness and Mitigation for police and security forces.

B. J. Srinath is a senior director (Scientist 'G') in the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology (IT), Ministry of Communications and IT, government of India. He is a specialist in the field of IT security management. He had a brief stint in Bharat Electronics Limited, Bangalore before moving to the government in 1991. He holds a degree in electronic engineering and is currently engaged in conceptualization and development of the National Cyber Security Strategy, and implementation of the National Cyber Security Assurance Framework. These programs are aimed at enabling protection of national critical information infrastructure and ensuring the safety and security of cyberspace in the country. Recently, he was nominated to represent India in the United Nations Group of Government Experts Committee and the Council for Security Cooperation in the Asia Pacific for studying "Developments in the Field of Information and Communication Technology in the context of International Security," and making suitable recommendations. He is also the national point of contact on behalf of the government of India to progress and coordinate with the world-wide Trusted Computing Initiative, comprising many countries and business leaders in the field of IT. In addition,

he has also represented India in the meetings of the Working Party on Information Security and Privacy of The Organisation for Economic Co-operation and Development in Europe. He is currently the chairman of a sectional committee of the Bureau of Indian Standards on information security and biometics for development of relevant international standards.

Lt. Gen. V. J. Sundaram (Retd.) is currently serving as the chairman of the board of governors of the National Design and Research Forum, and he is also an Honorary Professor at NIAS. He served in the Indian Army from 1957 to 1968, and also worked with DRDL from 1968 to 1997 in various positions of responsibility including as the chairman of the Indian missile program.

Lalitha Sundaresan is currently visiting professor at NIAS. She has a doctorate from the Indian Statistical Institute, Kolkata, where her work focused on digital processing of multisatellite data. She was a scientist at the Indian Space Research Organization, where she carried out studies to evaluate the usefulness of satellite remote sensing for monitoring natural resources and natural disasters with special reference to India. She worked as a principal scientific officer at DST, where she was involved with the setting up of Natural Resources Data Base centers in the districts of Karnataka. Together with IIT, Bombay, she was also involved in the development of the indigenous Geographical Information Software (GIS). She also coordinated training programs given by DST on the use of the Natural Resources Data Management System and GIS for development planning. Her recent works include the analysis of measurement errors in missile images obtained from open sources and the resulting impact of these errors on missile performance. She has also studied the Chinese university/research institution network and collaboration on superalloys as a critical part of the micro-level case study of Chinese capabilities in turbofan engine technology.

Vedpal Yadav has been working as lecturer in food technology since November 2000. Yadav has 10 published papers and 2 books. He has been working on food defense since 2008. Yadav participated in a United States Department of Agriculture (USDA)-Foreign Agriculture Service workshop on food defense at the National Center for Food Protection and Defense at the University of Minnesota in August 2013. He also participated in a 2-day workshop on food defense awareness in February 2013 at the HCM Rajasthan Institute of Public Administration in Jaipur organized by Federation of Indian Chambers of Commerce and Industry, Export Inspection Council of India, Food Safety and Standards Authority of India, USDA, and the U.S. Food and Drug Administration. He has delivered talks on food defense at various universities and institutes.

Abraham Verghese is Director, National Bureau of Agriculturally Important Insects, Bangalore. He is also the Editor of *Insect Environment.* Concurrently, he serves as the president of the Society for Biocontrol Advancement and is a

member of International Fruit Fly Steering Committee. Previously, Verghese held the position of head and principal scientist of entomology division at the Indian Institute of Horticultural Research in Bangalore. At the time, he was also the chief editor of *Pest Management in Horticultural Ecosystems* and member of Food and Agriculture Organization of the United Nations Phytosanitary Committee of Asia Pacific Plant Protection Commission. Apart from that, he served as the national project coordinator of the India-U.K. Fruit Fly Project. Verghese earned his Ph.D from London and a post-doctoral from Imperial College, London. He has participated in numerous special assignments and training programmes in India and abroad. In academia, he has held the position of post-graduate faculty in universities such as Agricultural Entomology, University of Agricultural Sciences, Kuvempu University, Bangalore University and Jain University. His work has been honoured with many awards in India and abroad, the most recent being Amulya Award for Innovation, Karnataka Government (2012) and Raitha Mitra Award, Mango Growers Hassan (2012). He has almost 35 years of research experience in pest management, ornithology and in advanced insect ecology. He has also published 200+ articles and journal papers in reputed international and national journals. Additionally, he has edited five professional books.

Appendix D

Biographical Sketches of the U.S. National Research Council Planning Committee Members

Norman R. Augustine (National Academy of Sciences [NAS], National Academy of Engineering [NAE]), *chair*, is the retired chairman and chief executive officer of the Lockheed Martin Corporation and a former under secretary of the army. Augustine served as a member of the President's Council of Advisors on Science and Technology and the Department of Homeland Security's (DHS) Advisory Council. He chaired the NAS committee that authored the report *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future*. Among Augustine's many honors are the National Medal of Technology and the Department of Defense's highest civilian award, the Distinguished Service Medal, given to him five times. He was awarded the 2005 American Association for the Advancement of Science (AAAS) Philip Hauge Abelson Prize and the 2006 Public Welfare Medal from NAS.

Augustine also served as chairman and principal officer of the American Red Cross for 9 years and as chairman of NAE, the Association of the United States Army, the Aerospace Industries Association, and the Defense Science Board. He is a former president of the American Institute of Aeronautics and Astronautics and the Boy Scouts of America. He is a current or former member of the Board of Directors of ConocoPhillips, Black and Decker, Procter & Gamble, and Lockheed Martin, and is a member of the board of trustees of Colonial Williamsburg, a trustee emeritus of Johns Hopkins, and a former member of the board of trustees of Princeton University and Massachusetts Institute of Technology. He holds 18 honorary degrees. Augustine graduated magna cum laude from Princeton University, where he earned bachelor's and master's degrees in engineering. He is the author of *Augustine's Travels*, *The Defense Revolution*, and *Augustine's Laws*.

Penrose (Parney) Albright was named the 11th director of Lawrence Livermore National Laboratory (LLNL), effective December 1, 2011. He is responsible for the management of the laboratory and also serves as the president of

Lawrence Livermore National Security, LLC. Albright has extensive experience in executive leadership, including policy direction, strategic planning, congressional and executive branch interactions, financial and personnel management of large mission-focused science and technology organizations, and research, development, testing, and evaluation of national security technologies and systems. Albright previously has served as the principal associate director for global security at LLNL.

Before arriving at LLNL, Albright was president of Civitas Group, LLC where he led projects to provide a net assessment of the nation's biodefense enterprise and conduct critical analysis of the first Quadrennial Homeland Security Review. The review created an analytic construct for setting priorities and making investment decisions that has been embraced by DHS leadership.

Prior to Civitas, Albright was confirmed by the Senate to the position of assistant secretary of DHS in 2003. His responsibilities included developing the multi-year strategic planning guidance and budget execution for the Science and Technology Directorate. This included new national efforts in radiological and nuclear security; biological, chemical, and explosives defense; boarder security, trade and travel facilitation; aviation, and other aspects of transportation security; national incident emergency response and consequence management; and critical infrastructure protection. Albright concurrently held the positions of senior director for research and development in the Office of Homeland Security and assistant director of homeland and national security within the Office of Science and Technology Policy. He was the lead official within the White House responsible for providing advice to the Executive Office of the President on science and technology issues surrounding homeland security, and on the threat of biological, nuclear, and chemical terrorism.

He previously worked at the Defense Advanced Research Projects Agency, where he developed and managed several programs associated with special operations, intelligence collection, molecular biology, communications, and maritime operations. He also worked as research staff at the Institute for Defense Analyses on ballistic and cruise missile defense systems; space-based infrared and launch-detection systems; and weapons and sensor system design and analysis.

John Holmes is deputy executive director of operations at the Port of Los Angeles, and oversees the Port Police, Port Pilots, Emergency Preparedness, Wharfinger, and Homeland Security divisions at the number one container port in the nation. Holmes holds the ultimate responsibility for Port-related security and public safety issues. His divisions work cooperatively with associated government and law enforcement agencies to uphold maritime laws, enforce safety and security regulations, and continually test and enhance emergency response and

preparedness procedures to ensure the safety of the Port workforce and residents in the surrounding harbor communities.

Holmes has 30 years of international management experience in a variety of positions that include chief operating officer, Fortune 500 executive, senior-level Coast Guard officer, and maritime security specialist. He most recently served as a principal and chief operating officer of the Marsec Group, a full-service security consulting firm specializing in supply chain security, technology, and operations. Prior to forming the Marsec Group, Holmes was vice president and director of business development for Science Applications International Corporation, where he assisted government and commercial customers with the development of technological solutions to homeland security challenges, with an emphasis on port, border, and military solutions.

Holmes retired from the United States Coast Guard in 2003 following 27 years of distinguished service in a variety of posts that included commanding officer, Officer in charge of marine inspection and captain of the port for the Los Angeles—Long Beach Port Complex. As Captain of the Port, Holmes was at the helm on September 11, 2001, and has been credited with swift and decisive actions that ultimately led to the creation of a number of national security initiatives, including the Maritime Transportation Security Act, Area Maritime Security Committee, and National Sea Marshal Program.

Earlier in his Coast Guard career, he served as deputy chief of the Coast Guard Office of Congressional Affairs in Washington, D.C., and as delegate and committee chairman at the International Maritime Organization in London. Holmes holds bachelor's degrees in English and education from Boston College, and a master's degree in business administration from Washington University's John M. Olin School of Business.

Nancy B. Jackson is manager of the International Chemical Threat Reduction Department in the Global Security Center at Sandia National Laboratories (SNL), which assists the U.S. Department of State and other federal agencies in solving problems related to international chemical security. With the Department of State, Jackson has developed the Chemical Security Engagement Program (CSP), an international program to raise awareness of chemical safety and security among chemical professionals and to enable the practice of safety and security in the research, teaching, and commerce of chemicals. CSP has worked with universities and small and medium chemical companies in Southeast Asia, South Asia, the Middle East, and North Africa. Her group is responsible for encouraging the safe and secure practice of chemicals in an effort to prevent their misuse as weapons, poisons, explosives, or environmental pollutants. This includes providing training in laboratory safety, process safety, and physical security.

Previously, Jackson was deputy director of SNL's International Security Program, where she assisted the director in fulfilling its mission to create technology-based solutions through international cooperation to reduce the threat of weapons of mass destruction (WMD) proliferation and terrorism. Prior to her positions in global security, Jackson was a principal investigator in heterogeneous catalysis with an emphasis on energy applications. Later work involved chemical imaging with a wide variety of applications from biological systems to homeland defense problems.

Jackson is a national affiliate of NAS where she has served on several boards and chaired studies. She is a fellow of AAAS and the International Union of Pure and Applied Chemistry and was recipient of the 2005 American Indian Science and Engineering Society Professional of the Year Award. In 2009, she was elected to the presidential succession of the American Chemical Society. She served as president-elect for 2010, president for 2011, and immediate past president for 2012.

She is a research associate professor at the Chemical and Nuclear Engineering Department of the University of New Mexico. Jackson has a B.S. degree in chemistry from George Washington University from which she won a Distinguished Alumni Achievement Award in 2005 and has a Ph.D. in chemical engineering from the University of Texas at Austin.

Randall S. Murch is the associate director, Research Development Team, National Capital Region at Virginia Tech. He is also a professor in practice in the School of Public and International Affairs and an adjunct professor in the department of plant pathology and physiology. He joined Virginia Tech in December 2004, where he develops research programs with special emphasis in topic areas in which science and technology, operations, law, policy, and security converge. Currently, his funded research activities are focused on advancing forensic science, biosecurity, and microbial forensics. He advises Ph.D. students in several graduate programs and teaches graduate courses in two programs. He has held a visiting professorship in the Science and Security Program in the department of war studies at King's College, London, and is currently a visiting faculty member at the Institute for Investigative Genetics at the University of North Texas Health Center in Ft. Worth, Texas.

Following completion of his Ph.D. and brief service in the U.S. Army Reserve, Murch's first career was with the Federal Bureau of Investigation (FBI), where he was a Special Agent. In his early years with the FBI, he was assigned to the Indianapolis and Los Angeles Field Offices, where he performed counterterrorism, counterintelligence, and other investigations. During his career, he was assigned to the FBI laboratory as a forensic biologist, research scientist, department head, and deputy director at various times. While department head and deputy director, he was instrumental in leading the overhaul of the FBI laborato-

ry. Also while in the FBI, he created the bureau's and United States' WMD forensic investigative program, served as the FBI's science advisor to the 1996 Olympic Games, led forensic investigative aspects of a number of domestic and international terrorism cases, and initiated a number of new and innovative programs for both the FBI laboratory and technical investigative program. Murch received his B.S. degree in biology from the University of Puget Sound in Tacoma, Washington, his M.S. degree in botanical sciences from the University of Hawaii, and his Ph.D. in plant pathology from the University of Illinois, Urbana-Champaign. He has published more than 40 scholarly papers, reports and chapters and has made numerous invited presentations as well as having testified in U.S. courts of law as an expert witness on more than 100 occasions.

Nancy Jo Nicholas has been a member of Los Alamos National Laboratory's (LANL) technical staff since 1990, and is the director of LANL's Nuclear Nonproliferation Program Office. From June 2006 to June 2010, she served as the LANL Nuclear Nonproliferation Division Leader responsible for 250 people who executed a significant nonproliferation mission. Prior to that she headed LANL's Nonproliferation and Security Technology Program Office, where she grew nuclear safeguards programs and helped place LANL personnel in key nonproliferation positions in Washington and Vienna. She previously served as deputy group leader for the LANL's Advanced Nuclear Technology Group helping manage an operational Cat I nuclear facility. She has served several assignments at the International Safeguards Division at DOE/National Nuclear Security Administration Headquarters and at the Rocky Flats Environmental Technology Site. Nicholas serves as vice chair of the Board of Directors and founding board member of WINS—the Vienna-based World Institute for Nuclear Security. She was elected and recently served a 2-year term as president of the Institute for Nuclear Materials Management, the premiere international professional society for nonproliferation and safeguards. She has extensive experience in both line and program leadership. Her technical field of expertise is nondestructive assay measurements. Nicholas earned a B.S. in mathematics and physics from Albright College and an M.S. in nuclear physics from George Washington University.

George Perkovich is vice president for studies and director of the Nuclear Policy Program at the Carnegie Endowment for International Peace. His research focuses on nuclear strategy and nonproliferation, with a concentration on South Asia, Iran, and the problem of justice in the international political economy. Perkovich is author of the award-winning book *India's Nuclear Bomb* (University of California Press, 2001) and co-author of the Adelphi Paper "Abolishing Nuclear Weapons," published in September 2008 by the International Institute for Strategic Studies. This paper is the basis of the book *Abolishing Nuclear Weapons: A Debate*, which includes 17 critiques by 13 eminent international commentators. He also co-wrote a major Carnegie report entitled "Universal Compliance: A Strategy for Nuclear Security," a blueprint for rethinking the

international nuclear-nonproliferation regime. The report offers a fresh approach to dealing with states, terrorists, nuclear weapons, and fissile materials to ensure global safety and security. He served as a speechwriter and foreign policy adviser to Senator Joe Biden from 1989 to1990. Perkovich is an adviser to the International Commission on Nuclear Nonproliferation and Disarmament and a member of the Council on Foreign Relations' task force on U.S. nuclear policy. Perkovich holds a B.A. in politics from the University of California at Santa Cruz, an M.A. in Soviet Studies from Harvard University, and a Ph.D. in Foreign Affairs from the University of Virginia.

Stephen Philip Cohen, *unpaid consultant*, has been senior fellow in foreign policy studies at the Brookings Institution since 1998. In 2004, he was named as one of the 500 most influential people in the field of foreign policy by the World Affairs Councils of America. Cohen was a faculty member at the University of Illinois from 1965 to 1998. From 1992 to 1993 he was scholar-in-residence at the Ford Foundation, New Delhi, and from 1985 to 1987, a member of the Policy Planning Staff of the U.S. Department of State, where he dealt with South Asia. He has taught at Andhra University (India) and Keio University (Tokyo), and Georgetown University, and now teaches in the South Asian program of Johns Hopkins School of Advanced International Studies. Cohen has served on numerous study groups examining Asia sponsored by the Asia Society, the Council on Foreign Relations, the Asia Foundation, and the National Bureau of Asian Research. He is a trustee of the Public Education Center. Cohen was the co-founder and chair of the workshop on Security, Technology and Arms Control for younger South Asian and Chinese strategists, held for the past 10 years in Pakistan, India, Sri Lanka and China, and was a founding member of the Research Committee of the South Asian strategic organization the Regional Centre for Security Studies, Colombo. Cohen has written, co-authored, or edited 10 books. Cohen received B.A. and M.A. degrees in political science from the University of Chicago, and a Ph.D. in political science from the University of Wisconsin. He has conducted research in Britain, China, Britain, Japan, India, Pakistan, and the former Soviet Union, and Japan. He received grants from several major foundations and serves as a consultant to numerous government agencies.

Appendix E

Biographical Sketches of National Institute for Advanced Studies Planning Committee Members

V. S. Ramamurthy, *chair*, is a well-known Indian nuclear scientist with a broad range of scientific and technical contributions from basic research to science administration. Ramamurthy started his career at the Bhabha Atomic Research Centre in Mumbai in 1963. His research focused on both experimental and theoretical fields, including nuclear fission and heavy ion reaction mechanisms, statistical and thermodynamic properties of nuclei, physics of atomic and molecular clusters, and low energy accelerator applications. From 1995 to 2006, Ramamurthy was fully involved in the promotion of science in India as Secretary to the government of India in the Department of Science & Technology (DST) in New Delhi. He was also the chairman of the International Atomic Energy Agency Standing Advisory Group on Nuclear Applications for nearly a decade. After retirement from government service, Ramamurthy, in addition to continuing research in nuclear physics at the Inter-University Accelerator Centre in New Delhi, was also actively involved in human resource development in all aspects of nuclear research and application. Ramamurthy is currently a chairman of the Recruitment and Assessment Board of the Council of Scientific and Industrial Research, and a member of the National Security Advisory Board. In recognition of his service to expand science and technology (S&T) in the country, Ramamurthy was awarded one of the top civilian awards, the Padma Bhushan Award, by the Government of India in 2005. Currently, Ramamurthy is the director of the National Institute of Advanced Studies (NIAS), Bangalore.

Manoj Bali, Scientist 'G' is the director of the Directorate of Low Intensity Conflict at the Defence Research and Development Organisation (DRDO) Headquarters (HQ). Bali completed his B.Tech (Mechanical) from the Thapar Institute of Engineering and Technology in Patiala in 1980. Following that, he joined DRDO at the Defence Research and Development Laboratory in Hyderabad as Scientist 'B' in 1982. In 1985, he moved to the Terminal Ballistics Research Laboratory in Chandigarh. In 2005, he joined the Group for Forecasting and Analysis of Systems and Technologies, and in 2007, moved to the Direc-

torate of Interaction with Services and Business at the DRDO HQ. Since 2009, Bali has worked in the Directorate of Armament. He has also focused on effectiveness analysis, time-cost overrun of projects, naval and army S&T requirements, the DRDO Materials Programme, the Soldier as a System Programme, and weapons requirements. He was sent to Annapolis, MD to study the American weapons acquisition process. Subsequently, he developed a defence acquisitions database for the Indian Defence Forces. He is a member of the High Energy Materials Society of India, the chairman of the joint DRDO-Air Force team for siting of underground storage for explosives, and the chairman of the Data Analysis Committee for the Delhi region. As a Member Secretary, he organised the national DRDO Golden Jubilee Student Competition for 2008 and 2009.

H. V. Batra, Scientist 'G' is the director of the Defence Food Research Laboratory in Mysore. Batra completed his M.V.Sc. and Ph.D both from Haryana University in 1977 and 1985, respectively. He worked as the head of the Mycobacteriology Department at the National Institute of Immunology in New Delhi from 1984 to 1990, and joined the Defence Research and Development Establishment in 1990. Batra has undertaken many technological innovations in the area of molecular biotechnology, immunoassay technology, construction of synthetic genes, and construction of chimeric genes/proteins. He achieved a breakthrough in hybridoma technology to rapidly generate specific high affinity monoclonal antibodies and has developed a number of diagnostic kits and systems for the detection of important biowarfare agents, which are extremely useful for onsite investigations of biological emergencies arising from natural outbreaks. He also prepared the Bio-defence programme for the country. Batra is a recipient of many awards, honours, and recognitions including the National Institute of Immunology Product Development Award in 1988, the DRDO Technology Cash Award in 1996, DRDO Scientist of the Year Award in 2002, and the Titanium Trophy Award in 2012. He has to his credit 134 publications in national and international publications, 12 chapters in national and international books, and nine patents. He has also guided 26 Ph.D. students. Batra is a life member of the Indian Immunology Society, a member of the Association of Veterinary Microbiology, an Immunologist and Specialist in Infectious Diseases, a member of the Veterinary Public Health Association, and a member of the Indian Leptospirosis Society.

S. Chandrashekar is currently a professor in the Corporate Strategy and Policy Area at the Indian Institute of Management Bangalore (IIMB). Prior to his joining IIMB he spent more than 20 years working at the Indian Space Research Organisation (ISRO). His work at ISRO covered all parts of the programme – satellite and rockets as well as the applications of space technology especially remote sensing. He was also involved with activities related to international cooperation and has represented and led Indian delegations to the United Nations Committee on the Peaceful Uses of Outer Space. His research interests at IIMB include technology and competitive advantage, national technology priorities

and national technology policy, studies on innovation, telecommunications in the Indian context, national innovation systems, modeling complex systems and national security issues. His most significant research contribution include analysis of technical and organisational aspects of China's missile capability; assessment of Pakistan missiles; and assessing the Indo-U.S. civil nuclear deal. His recent work includes a study of sensitive installations using open source satellite imagery. He has also been involved with other members of the group on a micro-level comparative case study of Chinese capabilities in one domain of technology related to the development of turbo-fan aircraft engine technology.

S. Gopal worked with the government of India for more than three and a half decades, during which he had wide experience in the analysis of national and international security and strategic affairs. After retirement, he was instrumental, along with other colleagues, in establishing the Institute of Contemporary Studies in Bangalore. The Institute started a quarterly journal called *Contemporary Analyst,* in which Gopal has been a regular contributor. One of his more important papers was on the Comprehensive Test Ban Treaty (CTBT), entitled "India and the CTBT." He is a member of the Asia Centre in Bangalore, where he presented a paper assessing Pakistan's security scenarios. In a seminar on Naxalism organised by the Observer Research Foundation in Chennai, he presented a paper entitled, "The Naxalite Movement: Impact of External Networking." In a seminar on Sri Lanka, recently organised by the Indian Centre for South Asian Studies and the Centre for Asia Studies, Gopal presented a paper entitled, "The Role of the Janata Vimukti Peramuna in Sri Lankan Politics," with particular reference to the ethnic question. Gopal also has wide experience in technical and imagery intelligence analysis.

Rajaram Nagappa is a specialist in aerospace propulsion and has worked extensively in the design and development of solid propellant rockets. His interests lie in missile technology and space weaponisation. He has served in the Vikram Sarabhai Space Centre at ISRO as its Associate Director, and later was the Pandalai Memorial Chair Professor at Anna University in Chennai. He has also taught at the Technion-Israel Institute of Technology in Israel. He is a recipient of the Astronautical Society of India Award, the Distinguished Alumnus Award of the Madras Institute of Technology, DRDO's Agni Award for Excellence in Self Reliance, the Certificate of Appreciation of the International Astronautical Federation, and the Honorary Fellowship of the High Energy Materials Society of India. His recent work includes an assessment of Pakistani cruise missiles and an assessment of the Iranian satellite launch vehicle *Safir*. He has also traced the development of fighter aircraft in China as a part of a study on China's S&T capability.

Gulshan Rai is director general of CERT-In (Indian Computer Emergency Response Team) and group coordinator of E-Security and the Cyber Law Division in the Ministry of Communications and Information Technology. Previously, he

was executive director of the Education and Research Network, India for over seven years and was instrumental in establishing the first large scale education and research network in close collaboration with the leading educational and research institutions in the country. Rai has worked since 1998 on the evolving legal framework to address issues arising from cyberspace. His sustained efforts in this area resulted in the second technology legislation in the history of India: the Information Technology Act and its recent amendments. Rai is particularly focused on developing security capabilities in the country through increased security education programs. He has initiated several programs in this area with industry and educational institutions. He has enhanced the security of government infrastructures through an effective security framework that prescribes standards, and is audited by a panel of independent auditors. Rai holds a Ph.D. and an M.Tech and has published several papers and reports on e-commerce, cybersecurity, cyber laws, education and networking, and has presented on these issues at several national and international conferences.

Anuradha Reddy is director of personnel in the Ministry of Defence. She has worked in the capacity of Officer on Special Duty to the Scientific Advisor to the Raksha Mantri from 2008 to 2012. Anuradha Reddy has a Ph.D. in international affairs from Jawaharlal Nehru University, is an alumni of the National Defence College of India and has studied trade negotiation at Harvard.

A. K. Sinha is a serving paramilitary officer from Sashastra Seema Bal and is presently working as senior research officer with the National Disaster Management Authority (NDMA). His current responsibilities include policy research, program planning, and interagency coordination in the field of chemical, biological, radiological and nuclear (CBRN) disaster management, including weapons of mass destruction and terrorism. With an M.V.Sc., he specialises in biological disaster management including bioterrorism and biosecurity. As a core group member, he has been associated with NDMA since its inception, and has contributed to the formulation of National Guidelines on Biological Disaster Management, Medical Preparedness and Mass Casualty Management, Management of the Dead in the Aftermath of Disaster, NDMA-World Health Organization Action Plan on Pandemic Preparedness Beyond Health and Plan to Counter the Threats to the Municipal Water Supply and Water Reservoirs. In addition to NDMA, he actively contributes to biorisk management capacity-building programs of DRDO, the Indian Council of Agriculture Research, the National Institute of Disaster Management, and the State Administrative Training Institutes. Sinha has expertise in biosecurity and bioterrorism. As a technical expert from NDMA, he has been associated with the Disarmament and International Security Affairs Division of the Ministry of External Affairs (MEA), and was also a member of the Indian delegation to the UN Biological Toxin and Weapon Convention (BTWC) in Geneva in 2008, the Biodefense Congress in Kualampur in 2011, the BTWC Review Conference in Geneva in 2011, and the Association of Southeast Asian Nations Regional Forum Workshop on Biorisk Management in

Manila in 2012. During his association with MEA and international exchanges, he contributed significantly to strengthening India's foreign policy obligations on global biorisk management. Currently Sinha is coordinating NDMA's Biological Disaster Management Programme and capacity-building programme on CBRN Prevention, Preparedness and Mitigation for police and security forces.

Lalitha Sundaresan is currently visiting professor at NIAS. She has a doctorate from the Indian Statistical Institute, Kolkata where her work focused on digital processing of multi-satellite data. She was a scientist at ISRO, where she carried out studies to evaluate the usefulness of satellite remote sensing for monitoring natural resources, and natural disasters with special reference to India. She worked as a principal scientific officer at DST, where she was involved with the setting up of Natural Resources Data Base centers in the districts of Karnataka. Together with IIT, Bombay, she was also involved in the development of the indigenous Geographical Information Software (GIS). She also coordinated training programs given by DST on the use of the Natural Resources Data Management System and GIS for development planning. Her recent works include the analysis of measurement errors in missile images obtained from open sources and the resulting impact of these errors on missile performance. She has also studied the Chinese university/research institution network and collaboration on superalloys as a critical part of the micro-level case study of Chinese capabilities in turbofan engine technology.