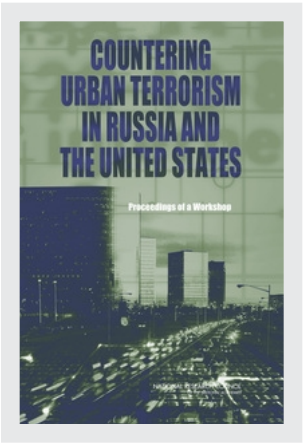
THE NATIONAL ACADEMIES PRESS

This PDF is available at http://nap.edu/11698

SHARE



BUY THIS BOOK

FIND RELATED TITLES

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

DETAILS

256 pages | 6 x 9 | PAPERBACK
ISBN 978-0-309-10245-2 | DOI 10.17226/11698

AUTHORS

Glenn E. Schweitzer and A. Chelsea Sharber, Editors, Committee on Counterterrorism, Challenges for Russia and the United States, Office for Central Europe and Eurasia, National Research Council, in cooperation with the Russian Academy of Sciences

Visit the National Academies Press at NAP.edu and login or register to get:

– Access to free PDF downloads of thousands of scientific reports
– 10% off the price of print titles
– Email or social media notifications of new titles related to your interests
– Special offers and discounts

Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. (Request Permission) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

Copyright © National Academy of Sciences. All rights reserved.

COUNTERING URBAN TERRORISM IN RUSSIA AND THE UNITED STATES

Proceedings of a Workshop

Glenn E. Schweitzer and A. Chelsea Sharber, *Editors*

Committee on Counterterrorism Challenges
for Russia and the United States

Office for Central Europe and Eurasia
Development, Security, and Cooperation
Policy and Global Affairs

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

In cooperation with the Russian Academy of Sciences

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

Copyright National Academy of Sciences. All rights reserved.

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

NOTICE: The project that is the subject of this report was approved by the 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 Grant No. B 7075.R02 between the National Academy of Sciences and the Carnegie Corporation of New York. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number 0-309-10245-6

A limited number of copies are available from the Office for Central Europe and Eurasia, National Research Council, 500 Fifth Street, N.W., Washington, DC 20001; (202) 334-2644.

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

Copyright 2006 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America.

Copyright National Academy of Sciences. All rights reserved.

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. Wm. A. Wulf is president of the National Academy of Engineering.

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

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

www.national-academies.org

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

NATIONAL RESEARCH COUNCIL COMMITTEE ON COUNTERTERRORISM CHALLENGES FOR RUSSIA AND THE UNITED STATES

Siegfried S. Hecker, Director Emeritus, Los Alamos National Laboratory; Visiting Professor, Center for International Security and Cooperation, Stanford University, *Chair*
Wm. A. Wulf, President, National Academy of Engineering, *Ex-officio*
Robert McC. Adams, Adjunct Professor, University of California at San Diego
John F. Ahearne, Director, Ethics Program, Sigma Xi, The Scientific Research Society
Lewis M. Branscomb, Aetna Professor of Public Policy and Corporate Management, Emeritus, John F. Kennedy School of Government, Harvard University
George Bugliarello, President Emeritus and University Professor, Polytechnic University
Anita K. Jones, Lawrence R. Quarles Professor of Engineering and Applied Science, University of Virginia
Michael Moodie, Independent Consultant and Former President, Chemical and Biological Arms Control Institute
Russ Zajtchuk, President, Chicago Hospitals International

National Research Council Staff

Glenn E. Schweitzer, Program Director
A. Chelsea Sharber, Senior Program Associate
Kelly Robbins, Senior Program Officer
Christopher Holt, Senior Program Assistant

RUSSIAN ACADEMY OF SCIENCES STANDING COMMITTEE ON COUNTERTERRORISM

Academician Yevgeny Velikhov, Director, Kurchatov State Research Center of Atomic Energy, *Chair*
RAS Corresponding Member Leonid Bolshov, Director, Nuclear Safety Institute of the Russian Academy of Sciences
Academician Nikolay Laverov, Vice President, Russian Academy of Sciences
Academician Nikolay Platé, Vice President, Russian Academy of Sciences
Academician Aleksandr Spirin, Director, Protein Institute of the Russian Academy of Sciences

Copyright National Academy of Sciences. All rights reserved.

Academician Konstantin V. Frolov, Director, Institute of Mechanical Engineering of the Russian Academy of Sciences
RAS Corresponding Member Valery Tishkov, Director, Institute of Ethnology and Anthropology of the Russian Academy of Sciences
Mr. Gennady Kovalenko, Presidium of the Russian Academy of Sciences
Dr. Renat S. Akchurin, Chief of the Cardiovascular Surgery Department, Cardiology Research Center

Russian Academy of Sciences Staff

Yury K. Shiyan, Chief Expert, Head of the Desk on Cooperation with North and Latin American Countries, Foreign Relations Department

Copyright National Academy of Sciences. All rights reserved.

Preface

This report presents the proceedings of the third U.S.-Russian interacademy workshop on the general theme of countering terrorism. The first report was published in 2002 under the title *High-Impact Terrorism: Proceedings of a Russian-American Workshop*. The second report was published in 2004 under the title *Terrorism—Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings*. The third report focuses on many important dimensions of urban terrorism, including the integration of response activities of different government organizations should a terrorist attack occur. The Carnegie Corporation of New York has generously supported all three of the workshops and the preparation of the reports.

The National Academies and the Russian Academy of Sciences (RAS) began cooperation in this field in 1999. In 2000, National Research Council (NRC) and RAS committees were established to lead the effort. The first workshop was then held in Moscow in June 2001. Since September 11, 2001, terrorism-related studies and other activities of the National Academies and the Russian Academy of Sciences have increased significantly, and the second and third reports have built on the expanded efforts on both sides of the ocean. The second workshop was also held in Moscow in March 2003. The third workshop was held in Washington, D.C., at the end of January and beginning of February 2005. This workshop was of particular interest since it included presentations by a number of specialists who have operational responsibilities for countering terrorism in each of the countries whereas presentations at previous workshops were made primarily by specialists who serve as advisers to governments.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Prior to the third workshop, three working groups of U.S. and Russian experts met to consider terrorism threats and responses associated with cybersecurity, ground transportation systems, and energy systems. These working groups had opportunities to meet with a number of U.S. specialists in each respective field and to visit facilities of particular interest in the Washington, D.C., metropolitan area. Appendix A sets forth the programs of the three working groups and of the plenary sessions of the workshop. Appendix A also identifies the U.S. and Russian participants in the workshop and the panels.

Following the workshop, the Russian specialists traveled to New York City where they had additional opportunities to become familiar with terrorism-related activities of fire, police, and transportation officials and specialists; review the events of September 11, 2001; inspect developments at Ground Zero; and discuss terrorism issues with specialists at Polytechnic University. The direct involvement of first responders in several of the meetings in New York was of particular interest to the Russian participants in the program. Appendix A sets forth the program in New York.

We have not attempted to summarize the papers that were presented at the workshop in these proceedings. We considered them to be of sufficient importance to be included in their entirety. The presentations and discussions during the working group meetings were summarized during the plenary session and these summaries are included. Included in Appendix B is a report of the activities of five subcommittees established by the NRC and RAS committees to consider various aspects of the terrorism challenge on a continuing basis, with progress reports presented at each workshop. These subcommittees address radiological terrorism, biological terrorism, cyberterrorism, urban terrorism, and the roots of terrorism.

ACKNOWLEDGMENTS

As noted above, this publication was made possible by a grant from the Carnegie Corporation of New York. The statements made and views expressed are solely the responsibility of the authors and do not necessarily represent the positions of the Carnegie Corporation, the National Academies, the Russian Academy of Sciences, or other organizations where the authors are employed.

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

We wish to thank the following individuals for their review of selected papers: Dorothy Denning, Naval Postgraduate School; James Hill, National

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Institute of Standards and Technology; Darleane Hoffman, University of California at Berkeley; Martin Hugh-Jones, Louisiana State University; David McIntyre, Texas A&M University; Paul Pillar, Georgetown University; Charles Tilly, Columbia University; and William Wallace, Rensselaer Polytechnic Institute. Although the reviewers listed above have provided constructive comments and suggestions, they were not asked to endorse the content of the individual papers. Responsibility for the final content of the papers rests with the individual authors.

Special thanks are extended to Kelly Robbins for her translation of the Russian language papers into English and to Jan Dee Summers for her work in editing these proceedings.

Siegfried S. Hecker
Chair, NRC Committee on Counterterrorism Challenges for Russia and the United States

Glenn E. Schweitzer
Director, Office for Central Europe and Eurasia, National Research Council

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

Contents

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

Report of U.S.-Russian Working Group on Energy Vulnerabilities

Aleksandr Yu. Kudrin, Edward V. Badolato, Sergey G. Vasin, Benjamin S. Cooper, Glenn E. Schweitzer

On January 27-28, 2005, the National Academies-Russian Academy of Sciences Working Group on Energy Vulnerabilities met in Washington, D.C., to discuss energy systems vulnerabilities in conjunction with terrorist attacks.

PRESENTATIONS TO THE WORKING GROUP

The working group met with representatives of the U.S. Department of Energy, the Board on Energy and Environmental Systems of the National Research Council, the American Petroleum Institute, and the Edison Electric Institute.

The discussion with the U.S. Department of Energy considered the events that triggered the northeast power blackout of 2003, which affected 50 million consumers of electricity in the United States, and the actions that have been taken to reduce the likelihood of future power blackouts. Four factors contributed to the blackout: (1) inadequate understanding among the operating organizations of the overall system, a shortcoming that was responsible for a lack of appropriate voltage criteria and a lack of effective remedial measures for contingencies; (2) inadequate situational awareness among operators who did not realize that system conditions were degrading; (3) inadequate tree trimming under transmission lines that led to the first three line failures; and (4) inadequate diagnostic support that failed to detect growing overloads.

The relevance of this incident, and particularly the ripple effects, to a terrorist attack on power systems is significant. While there are many vulnerabilities in power systems, precautions that should be taken to minimize damage from an attack by terrorists are quite analogous to precautions taken to prevent outages from hurricanes and other natural disasters. There is a special concern that ter-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

rorist attacks on power systems might be coupled with other types of terrorist attacks, particularly in large cities. Finally, vulnerabilities of control systems to cyber- and physical attacks need special attention.

The Board on Energy and Environmental Systems of the Division on Engineering and Physical Sciences of the National Research Council also provided briefings on relevant activities and studies. Three overriding concerns regarding terrorist attacks on energy-related systems are (1) electrical systems, especially transmission network substations; (2) petroleum refineries, which if attacked could threaten nearby residents although the overall impact would be less than an attack on an electrical system; and (3) gas pipelines, which if attacked could also threaten nearby residents, but again would have less impact than disrupted electrical systems. Among the approaches to protect electrical systems are physical barriers around critical components, modular extra-high-voltage transformers, improved surveillance technologies, and adaptive electrical grids that limit cascading failures. Relevant studies currently under way address the safety and security of commercial spent nuclear fuel storage and enhanced resilience of electric transmission networks. A study of safety at liquefied natural gas facilities may soon be launched.

The discussion with the American Petroleum Institute centered on security vulnerability assessment methodology for the petroleum and petrochemical industries. The assets of concern include 4,200 offshore oil platforms, 100 U.S. ports, 148 refineries, 160,000 miles of liquid pipelines, 35,000 gasoline tanker trucks, 7,500 bulk storage plants, and 170,000 service stations. Important concepts include definition and prioritization of risks, types of direct and indirect consequences of an attack, attractiveness to terrorists of different assets, threat scenarios involving groups with different motivations, and vulnerabilities in protection of different types of assets. The methodology should give considerable attention to countermeasures that can be employed, including consideration of cost and vulnerability tradeoffs. Various sources of data were discussed, and the relevance of previous experiences in countering all types of threats was emphasized. Finally, the types of personnel injuries, economic losses, and environmental damage that must be anticipated were highlighted. The importance of individual companies working with local law enforcement officials is obviously of utmost importance given the wide variation in facility types and locations.

The emphasis during the discussion with the Edison Electric Institute was on the working relationships between the private sector and the government (both federal government organizations and local agencies). Industry includes federal utilities, investor-owned utilities, municipal and state utilities, and rural electric cooperatives. The North American Electric Reliability Council provides an important umbrella organization for addressing standards and methodologies for countering threats of terrorism. At the same time, the U.S. Congress is concerned about insurance coverage, regulations and mandatory standards, and frequency allocations. The U.S. Department

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

of Homeland Security interacts with the private sector in many ways, including sharing data, conducting emergency exercises, and promoting interoperability. Other government agencies also have continuing interactions with the private sector in the energy field, and particularly the U.S. Department of Energy and the Federal Energy Regulatory Commission.

In addition to discussions with outside organizations, the members of the working group themselves described the activities in which they are directly involved. The presentations of the working group members addressed pipeline security planning; protection of critical physical infrastructure, particularly key facilities, on a broad scale; development of standards and regulations at the national level; and practical challenges in preventing terrorist incidents in a large city, with special attention to the challenges of monitoring activities involving vehicular traffic.

In summary, the working group considered a broad range of issues in the energy sector. As suggested above, emphasis was given to protection of functional infrastructures, particularly pipelines, petroleum assets, and power generation and distribution; crosscutting concerns, including threats, vulnerabilities, preparedness, and determination of risk; and practical experience in applications of technologies and in dealing with government structures. Nuclear energy was given only minimal attention in view of the many unique challenges and experiences encountered in this sector. Finally, while relevant U.S. research and development efforts were considered, discussion of Russian research and development activities was left to other groups with more expertise in the area.

TOPICS FOR FURTHER CONSIDERATION

The working group highlighted three topics that deserve more detailed consideration, within national and international contexts. These topics are of great importance in the United States and Russia, and improved understanding of recent developments should be of mutual interest to specialists from both countries.

First, vulnerability assessments are playing a large role in developing plans to reduce damage from terrorist attacks. However, there are shortcomings in attempting to develop generic vulnerability assessments, or even assessment methodologies, given the wide variations in types of terrorist scenarios and types of facilities at risk. The breadth of application of specific types of vulnerability assessments deserves detailed consideration. Also, development of approaches in adapting generic assessment frameworks to specific problems is important, and this topic should be further pursued.

Second, the role of government is central to all efforts to counter the threat of terrorism. Many of the most worrisome scenarios cut across the responsibilities of individual government agencies, and coordination is of high priority. Also, as previously discussed, clarification of the respective roles of government

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

and the private sector is important, and the integration of efforts needs continuing attention. While the histories of governmental control and the current configurations of the private sector vary considerably when considering the United States and Russia, improved understanding of the role of government in each country is critical if effective cooperative efforts are to be undertaken.

Finally, the emergency response systems in Russia and the United States are of critical importance in limiting damage from terrorist attacks. In many respects these systems should be multipurpose and capable of responding to all types of emergencies. However, there are unique problems posed by terrorist attacks, including the possibility of multiple attacks at one target or at dispersed targets and the design of attacks to cause fear as well as death and physical damage. The accumulation of experience around the world in responding to attacks can be valuable to all governments.

NEAR-TERM STEPS FOR BILATERAL COOPERATION

Several of the many topics that might be considered in developing cooperative programs were singled out for special attention, for example:

- **Reciprocal observation of and participation in simulations of terrorist attacks.** Simulations have been held and are being planned in both countries. Opportunities to participate in such exercises would be an excellent way to share experiences in the practical aspects of coping with terrorism.
- **Joint development of methodologies and standards for vulnerability assessments, priority ranking of critical facilities, and assessments of adequacy of protection.** Each of these topics is at the heart of efforts to counter terrorist attacks in urban areas. In-depth cooperation focused on any one of the topics should uncover lessons learned of mutual interest.
- **Cooperation in the development of sensors and other technical means for monitoring facilities and transportation.** Both countries have strong technical capabilities of direct relevance to counterterrorism efforts, particularly in the field of sensors. A review of selected arrays of sensors that each country has developed but that are not excessively sensitive and the operating experience using these sensors would be a good first step in developing cooperative programs.
- **Improving understanding of government-private sector collaboration.** Specialists in each country have difficulty understanding how the government structure and the private sector function in the other country. Since the role of government is central to almost all counterterrorism activities and since much of the burden of implementing preventive strategies falls on the private sector, improved familiarity with organizational responsibilities and practical experiences would be of benefit to many specialists in the two countries.

Copyright National Academy of Sciences. All rights reserved.

Report of U.S.-Russian Working Group on Transportation Vulnerabilities

Mortimer L. Downey, Nikolay A. Makhutov, Robert E. Gallamore, Konstantin V. Frolov, Kelly Robbins

On January 27-28, 2005, a group of U.S. and Russian experts met at the National Academies in Washington, D.C., to discuss a wide range of issues connected with the vulnerabilities of the transport system to terrorist threats. Working group participants and guest speakers discussed technical, legal, social, and economic aspects of the problem and visited the Washington Metropolitan Area Transit Authority headquarters and Maryland State Highway Administration control center to gain practical insights from personnel in the field.

The working group concluded that responses to terrorist attacks must be based on robust capabilities to respond to natural and technogenic disasters that should already be in place at the local and national levels. Efforts to prevent and respond to terrorist attacks do not require the establishment of separate systems but should be integrated into and complement existing emergency response capabilities.

TYPES OF TERRORISM ACTIVITIES CONSIDERED: THREATS, VULNERABILITIES, AND SCENARIOS

The Russian and U.S. participants identified the great risks and vulnerabilities inherent in many transportation systems in the urban environment. The same factors that make for an effective transportation system also create significant vulnerabilities. The participants also identified the importance of effective risk assessment and prioritization in addressing these threats, as well as threats posed by cyberattacks or attacks on the energy system that supports transport.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- Urban transport (buses, subways, commuter rail, water transport, automobiles, and trucks)—In order to be functional open systems with free access, a substantial risk is incurred, since these systems have such a high concentration of users. Motor vehicles are an even greater risk, since their flexibility of movement allows them to serve as effective weapons delivery systems.
- Railroads—The wide extent of rail facilities, their open and unprotected nature, and their use in transporting hazardous materials that are essential to urban life, such as the chlorine used for water purification, also makes them an attractive target.
- Urban ports—Container movements are the key to low-cost movement of concentrations of goods in international trade, but containers are equally effective carriers of weapons of mass destruction. Similar concerns exist about energy transportation facilities, particularly the handling of liquefied natural gas.

Terrorist attacks in the transport environment can take a number of forms, further complicating the task of prevention and response. Among the forms are

- vehicles used as weapons to deliver explosives or other materials against a target
- attacks on a transport vehicle and its passengers
- attacks on transportation facilities, such as railway or bus stations, where large numbers of passengers may congregate
- attacks on transportation infrastructure, such as bridges, railbeds, or signal systems; these attacks could include cyberattacks on transportation control systems

OVERVIEW OF GOVERNMENT EFFORTS

While there is much to be done, governments are taking steps to develop a response to the risk of terrorism, using a variety of methods, including the application of technology, such as

- investments in security systems—systemwide improvements to track and protect the movements of goods and people
- technology development—new technologies to detect and, where possible, protect against explosives, chemicals, and other weapons in the urban setting
- regulatory measures—new rules for the movement of hazardous materials, handling of containers, information flows about movements, and so forth
- improved response capability—steps to train, equip, and improve the capabilities of first responders, transportation system employees, and the public as a means of mitigating the impact of terrorist actions

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

PRIORITIES FOR THE ACADEMIES

The transportation systems vulnerabilities working group identified several priorities for the U.S. National Academies and the Russian Academy of Sciences, including systems research, basic research, technology development, consequence management, and social science research.

Greater attention to the overall effectiveness of transportation systems and terrorism countermeasures with particular reference to improvements that can provide both economic and security benefits is a priority for the academies. Encouraging basic research that can provide new tools to identify and interdict weapons is also a priority.

Technology development includes the utilization of research findings to develop new technology that is workable in field deployment. This process must be based on fundamental interdisciplinary research, leading to applied research, and finally to the development of specific systems and devices.

Consequence management encourages research into such issues as postattack cleanup and standards for exposure to various agents. It is necessary to reach consensus on standards and means of monitoring for adequate and acceptable levels of exposure and cleanup. The potential use of chemical substances as terrorist weapons represents a major paradigm shift, increasing their dangers and altering the existing understanding of allowable dose levels and consequences of exposure, and this shift requires a fundamental reconsideration of these issues.

Social science research recognizes the difficulties in total prevention of terrorist incidents in the current environment. Research attention is needed to better understand the causes of terrorist actions and the ways in which basic drivers of terrorism can be displaced.

PAST AND CURRENT ACTIVITIES OF THE U.S. NATIONAL ACADEMIES

The U.S. National Academies Transportation Research Board (TRB) has a Standing Committee on Critical Transportation Infrastructure Protection. TRB also administers extensive cooperative research programs that support research on a range of relevant issues, including development of training courses and manuals for first responders and transport system personnel for use both in their strategic planning efforts and in deployment of their operational resources.

AREAS OF COMMON INTEREST

There are many areas of common interest for the U.S. National Academies and the Russian Academy of Sciences, particularly in the social science field and in applying interdisciplinary thinking to the response to and resolution of terrorist acts. Both academies recognize the need for a greater focus in research activ-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

ities and coordination of work undertaken in government, scientific institutions, and industry.

Security considerations should become a key factor in the design of infrastructure and systems (including tunnels, underground parking structures, and elevated rail systems, as well as the transport system elements mentioned above), and should incorporate continual review of the implications of new systems and improvements as they are put in place.

Taking the next steps in interacademy cooperation will be facilitated by

- continuation of periodic information exchange
- cooperation in research
- joint expert analysis in order to provide independent opinions regarding major, promising projects for the development of transport systems

OBSERVATIONS

Priorities for continued bilateral cooperation include

- encouragement of research priorities as noted above
- sharing of intelligence with local and regional agencies (local agencies and transport systems personnel need access at some level to information about potential threats)
- development of independent research institutes and red teams to evaluate strategies and responses
- development of standards, methodologies, and data sources for risk assessment studies at a level of investment related to the amount of potential damage and the relationship of the funding of studies to the economic consequences of terrorist incidents; more study is required to establish the level of expenditure that would be appropriate (possibly in the neighborhood of 1 percent of project cost) and to identify potential sources of funding for these costs
- more financial support for equipment, training, and other needs of first responders, transportation system employees, and the public

Copyright National Academy of Sciences. All rights reserved.

Report of U.S.-Russian Working Group on Cyberterrorism Issues

Anita K. Jones, Igor Fedorov, Lewis M. Branscomb, Nikolay V. Medvedev, Yury K. Shiyan, Linton Wells III, Michael Wolin, A. Chelsea Sharber

The National Academies-Russian Academy of Sciences Working Group on Cyberterrorism Issues held discussions and consultations in Washington, D.C., on January 27 and 28, 2005. Experts from institutions in Moscow and the United States comprised the working group.

The working group visited the U.S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD) and the D.C. Emergency Management Agency and received briefings from the CERT Coordination Center (CERT/CC) at Carnegie Mellon University and the National Academies Computer Science and Telecommunications Board. In addition, working group members made presentations on current and past activities in the United States and Russia on the contribution to security from work in the field of computer science. These activities include several National Academies reports, the 2003 Conference on Grand Challenges in Information Security and Assurance, the curriculum for the six-year program to train cybersecurity specialists at Bauman Moscow State Technical University, and advancements to incorporate cybersecurity into Russian government policy and legal framework.

SITE VISITS

U.S. Department of Homeland Security National Cyber Security Division (NCSD). The working group became acquainted with NCSD's mandate, which is shared with U.S. Computer Emergency Readiness Team (U.S.-CERT) and described in the publications *National Strategy for Homeland Security*[1] and

[1]Office of Homeland Security. 2002. National Strategy for Homeland Security. Washington, D.C.: The White House. See http://www.whitehouse.gov/homeland/book/.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

The National Strategy to Secure Cyberspace.[2] The working group also learned about NCSD's priorities and mission—to secure cyberspace and U.S. cyberassets by implementing the strategy outlined in *The National Strategy to Secure Cyberspace* and priority protective measures to reduce the cybervulnerabilities of U.S. critical infrastructures. NCSD is divided into four organizational components: (1) U.S.-CERT operations, (2) outreach and awareness, (3) strategic initiatives, and (4) law enforcement and intelligence coordination.

NCSD's international objectives include international cooperation with industry and critical infrastructure sectors; increased computer security incident response capabilities through training and technical assistance, adoption and implementation of principles described in *OECD Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security*;[3] and encouragement of other countries' acceptance of the Council of Europe Convention on Cybercrime or individual laws at least as comprehensive (this becomes relevant when criminals are not physically within U.S. jurisdiction). Finally, the NCSD seeks a balance among government policy makers, law enforcement, and computer security incident response teams for international cooperation and collaboration.[4]

CERT Coordination Center. The CERT/CC connection to DHS was discussed, as well as trends in cybercrime. The malicious codes created to disturb the cyberenvironment are becoming more sophisticated. As a result, it is no longer possible to separate physical security and cybersecurity. Whether cyber or criminal threats are made, a better categorization than *malicious activity in cyberspace* needs to be created for them.[5]

D.C. Emergency Management Agency/Emergency Operations Center. The working group visited the Emergency Operations Center (EOC) of the D.C. Emergency Management Agency. Before September 11, 2001, the EOC was much smaller, with only 24 seats available for various response and critical infrastructure organizations. Not all of these seats had computers, and the computers that were in place were networked to one another but not outside the building. Since September 11, 2001, the EOC has been remodeled and can seat 50–60 representatives of the relevant response and critical infrastructure organi-

[2]The Whitehouse. 2003. The National Strategy to Secure Cyberspace. Washington, D.C.: The White House. See http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[3]Organisation for Economic Co-Operation and Development. 2002. OECD Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security. Paris, France: OECD.

[4]Information taken from a presentation, National Cyber Security Division and U.S.-CERT—Overview, made by Liesyl Franz, Public Policy and International Affairs, National Cyber Security Division, U.S. Department of Homeland Security, on January 27, 2005 to the U.S.-Russian Working Group on Cyberterrorism Issues.

[5]Information taken from a presentation to the U.S.-Russian Working Group on Cyberterrorism Issues by Casey Dunlevy, CERT/CC, January 28, 2005.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

zations. It is connected to the D.C. power grid and has backup battery power, a backup generator, and analog telephones in case of power failure. Weekly tests are conducted on the generator. In addition, two backup sites and two mobile command vans are available. This remodeled site, however, will soon be replaced by a completely new EOC located at a new site in D.C.

In addition to housing and managing the EOC, the D.C. Emergency Management Agency works with the community to provide current information on emergency situations and current guidelines on action in an emergency. This includes the Alert D.C. Program, a voluntary program that allows D.C.-area residents and employees to receive emergency communications as text messages, voice alerts, or radio broadcasts, and publications such as *It's a Disaster! . . . and What Are YOU Gonna Do About It? A Disaster Preparedness, Prevention, and Basic First Aid Manual*.[6]

PRIORITIES FOR THE FUTURE

The working group considered the following important priorities for future investigation.

Development of cooperative and complementary research programs to develop new principles, methods, and tools to design and construct more dependable systems; to quantify system attributes and risk (metrics); and to prevent, detect, and recover from cyberattacks. The working group believes that the rate of research progress to develop more dependable and robust systems is far short of what is needed. Further, without metrics to quantify both costs and benefits of reducing vulnerability to cyberattack, markets for those tools will continue to be weak.

Explore the most effective approach for developing national and international policy and law for cybercrime and cyberterrorism. In order to develop policy, it is important to examine the need for a common glossary of terms for international use in laws and regulations, jointly developed by legal and technical experts, and to explore how the academies can facilitate the solution of these problems.

Legal and regulatory structures for suppressing cyberattacks are fragmentary, inconsistent in terms and language used, and incompatible across national boundaries. Progress to rectify these shortcomings is urgent. A good place to start is a common set of terms for the methods of cyberattack, agreed to internationally by technical and legal experts.

[6]Liebsch, B., and J. Liebsch. 1999. It's a Disaster! . . . and What Are YOU Gonna Do About It? A Disaster Preparedness, Prevention, and Basic First Aid Manual. Tucson, AZ: Fedhealth.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Develop and exchange curricula for cybersecurity education and training. Cybersecurity education, based on a solid computer science foundation and including at least two postgraduate years of advanced and practical work, is essential to staff the vulnerable institutions and meet the need to develop better tools and methods. The main goals for specialist training include

- developing a security policy based on international and national standards
- using international standards to analyze information security risks
- developing a network traffic security policy
- applying techniques of information security identification and elimination of information security threats
- implementing techniques of information security based on international and national standards
- identifying information security risks
- modeling attacks and protection technologies
- auditing information security systems

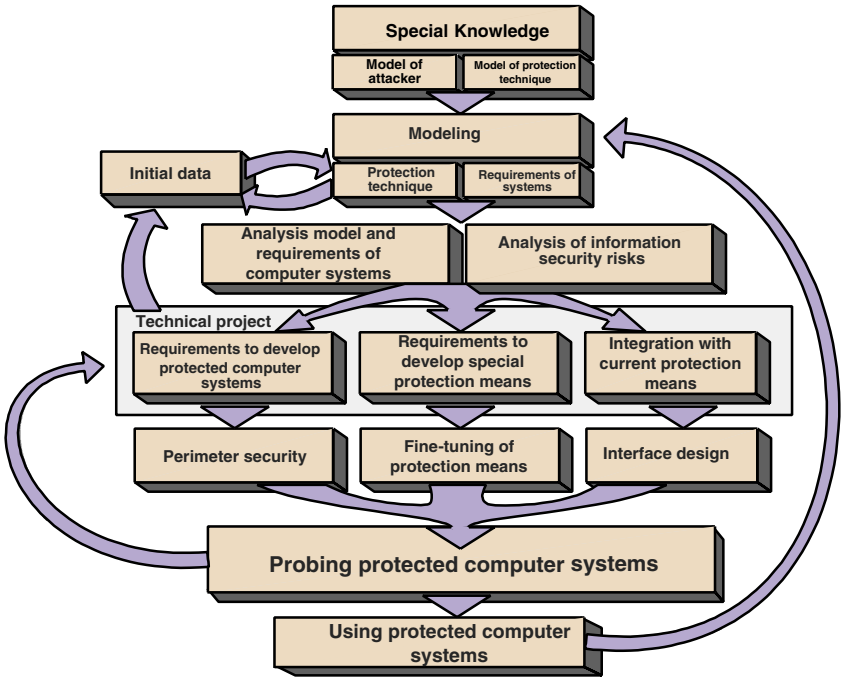


FIGURE 1 Skills for cybercrime prevention specialists at Bauman Moscow State Technical University.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

The six-year program at Bauman Moscow State Technical University provides an interesting model for cybereducation and cybertraining. Figure 1 shows how different elements of education relate to each other.

Enable exchange visits of university scholars studying cybersecurity. The working group believes that academic exchanges are the best way to get experience with alternative curricula for cybersecurity. Summer internships and programs for students (graduate and undergraduate), instructors, and researchers are included in this possibility.

Copyright National Academy of Sciences. All rights reserved.

Cybersecurity and Urban Terrorism—Vulnerability of the Emergency Responders

Anita K. Jones, Linton Wells III, Michael Wolin

During any type of crisis, the inhabitants of an urban area rely on emergency services provided by the government. Emergency responders remove or reduce the cause of the crisis, where possible, and also provide protection and aid to those affected. To do so, emergency services must take timely, coordinated, and appropriate action. They make use of critical information that must be accessed and transmitted to a variety of irregular players along uncertain channels. At any time, emergency services are vulnerable to disruption by groups using cyberattacks, but during a time of intense emergency, this vulnerability is heightened. During a crisis, normally autonomous emergency responders must by necessity act coherently and cohesively. This requires a dynamic and ad hoc flow of information. Because the emergency responders themselves are crucially dependent on information, a coordinated and well-executed cyberattack could degrade effective emergency response.

This cyberthreat causes emergency responders to be at risk from a common tactic used by terrorists—that is, to amplify a main attack with a supporting attack. After a main attack, terrorists might make a secondary assault on assembled emergency responders or their supporting information systems. This could reduce their ability to respond and possibly create more casualties. A secondary cyberattack may be employed before or coincidentally with a physical attack to impede effective deployment of emergency responders and thus amplify the damage from the physical attack. If the public were to perceive that the emergency response service were crippled or inoperable, terror among citizens is likely to be substantially increased. Both individual emergency response organizations and entire emergency systems must be defended against cyberattacks while at the same time the ability of the individual organizations to communicate and coordinate action is not impeded.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

This paper examines the emergency response to a terrorist attack on an urban area by viewing it as a system that is vulnerable to disruption. It focuses on the critical aspects of emergency response that are at risk of being impeded by an attack on the computer or telecommunications networks of the emergency responders themselves. It examines the possible cybertactics a terrorist group may use to amplify the effects of a physical attack by limiting emergency response.

CRITICAL INFORMATION

In any emergency there is a wide array of critical information that is central to an effective response. Some of this information is general in nature and commonly possessed by highly trained emergency response units, but much of it will be specific to the time, location, and type of attack. This critical information forms the input information that any emergency response system must possess to effectively respond to the situation.

This critical information includes, but is not limited to, building blueprints and city utility plans, crisis response plans, chemical cleanup procedures, treatments for specific biological or chemical agents, duty rosters and personnel contact information, individual victim medical records, and public announcements. One of the frustrating aspects of emergency preparation is how much detailed situation-specific information becomes critical to operational success. There is a wide array of different, relevant kinds of information, and some of these data inputs are voluminous.

By its nature a cyberattack will be against the content, accessibility, or flow of critical information. Because some of the needed information is incident specific, some information is accessed in (close to) real time. Because the attacker is aware of the specifics of the attack, and can deduce what information will be most helpful to responders, prearranged corruption of this information is a threat.

EMERGENCY RESPONSE PLANS FOR URBAN AREAS IN THE UNITED STATES

Urban areas are especially vulnerable to high-profile attacks because of the concentration of people, resources, and critical infrastructure in a small area. Hence most urban areas in the United States have developed emergency response plans that define how the various emergency services and government agencies will interact and work together during a crisis. For Washington, D.C., this plan was created by the D.C. Emergency Management Agency and is titled the District Response Plan (DRP).[1] The DRP describes how D.C. agencies will

[1]This plan is available on the D.C. Emergency Management Agency web site: http://dcema.dc.gov/dcema/cwp/view,a,1226,q,533529,dcemaNav,l31810l.asp.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

work collaboratively within the city and with regional and federal partner organizations in an emergency. In this paper the DRP is used as a representative example of urban emergency response plans in the United States.

At its heart the DRP identifies 15 emergency support functions. Each one is a vital task that the government must perform during an emergency response. Functions include transportation, firefighting, medical services, urban search and rescue, law enforcement, and media relations.[2] The DRP defines the city agencies and departments that have a part to play in each function. It then outlines the purpose and scope of each function and in what ways each organization will be involved and finally, how operations will proceed for each function.

The 15 functions can be seen as the spokes of a wheel with the D.C. Emergency Management Agency at the hub of the wheel. Operating out of the agency's Emergency Operations Center (EOC), the central emergency management decision makers will coordinate the actions of these largely autonomous emergency support functions. Responding to any emergency will require many different types of emergency services. For example, responding to a simple building fire requires firefighters to put out the flames, emergency medical care providers for the victims of the fire, and police officers to secure the area and control the flow of traffic around the area. In large-scale crises, a larger variety of services will be required—all at the same time. For an effective response to an emergency, the central EOC must efficiently and effectively coordinate the actions that support the emergency support functions.

While at the planning stage, the responders should give thought to the alternative technologies they would elect to use. In Tokyo, for example, the first responders and a network of decentralized command and control officials use VHF (very high frequency) radios, which, unlike cellular phones or wired phones, are relatively invulnerable to both physical and cyberattacks, although they can be jammed. Plans should consider the vulnerabilities inherent in the technologies used.

EMERGENCY RESPONSE

Emergency response in an urban environment on a large scale has several key aspects, all of which rely on the deployment of information technology, and thus may be vulnerable to attack. These aspects are a timely response, preplanned and coordinated operations, informed responses, and assured communication. This paper discusses each aspect in turn, with an emphasis on its vulnerabilities to cyberattacks.

[2]For a full list, see p. 2 of http://dcema.dc.gov/dcema/lib/dcema/info/pdf/basic.pdf.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TIMELY RESPONSE

The speed at which an emergency response is initiated can be critical. In crisis situations the presumption is that delay costs lives. A rapid arrival of the appropriate responders depends upon identification of the nature of the emergency, the notification to responders that an identified form of crisis exists, acknowledgment by those responders that it must be acted on, preparation by the responders for the appropriate response, and finally, rapid transportation to the crisis location.

There are a number of ways in which cyberattacks could be used to delay the arrival of emergency responders. Terrorists might try to delay notification of the crisis by misdirecting the initial notification, misrepresenting a critical need, or hindering the mobility of the first responders. The first two means of attack usually center on tampering with the notification system that citizens use to call upon the government and emergency services for aid. In the United States this is predominantly the 9-1-1 telephone system that is answered 24 hours each day by government-paid emergency response operators. Terrorists could use a computer attack against the functioning of this system or might inject a false alarm in order to erroneously send responders on misleading emergencies, thus evoking skepticism when a true emergency occurs.

A more direct attack on the 9-1-1 system may be to sabotage the system outright, hindering the ability of the public to directly connect with representatives from the emergency services system. This was accomplished on a limited scale by a Swedish hacker in 1997. He used a denial-of-service attack to jam the 9-1-1 emergency telephone lines in west-central Florida. From Sweden he accessed the telephone network and generated 60,000 unauthorized calls. This served to block access to the 9-1-1 service for Florida residents with real emergencies. In addition, the hacker diverted 9-1-1 calls to other destinations and harassed the 9-1-1 operators. He was tried as a juvenile in Sweden and fined the equivalent of $345.[3] This example demonstrates that the 9-1-1 system in the United States is vulnerable to cyberintrusion. Such an attack could originate from any point on the globe and could effectively cripple the ability of citizens to solicit aid from the emergency responders.

Another possible attack could involve falsifying the type of danger, leading the responders to prepare and deploy unnecessarily, or to arrive ill-equipped for the real emergency so that taking appropriate action on site is unduly delayed. This could be accomplished by planting false 9-1-1 calls or by falsifying the information flowing from 9-1-1 operators to emergency service organizations.

A final possible attack involves hindering responders on their way to the emergency. This might include co-opting supervisory control and data acquisi-

[3]Correll, John T. 1998. War in Cyberspace. Air Force Magazine 81(1). See http://www.afa.org/magazine/Jan1998/0198warin_print.html.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

tion (SCADA) systems for traffic signals to increase traffic congestion along routes to the emergency, or to even reroute the path taken by the responders so that it takes longer to arrive.

Plans should include provision to understand the nature of problems. For example, authorities should be able to determine where excess traffic on phone lines is due to a denial-of-service attack or legitimate attempts by citizens to communicate with authorities.

PREPLANNED AND COORDINATED OPERATIONS

The response to an emergency situation will usually take the following form: preplanning, implementation of that plan, and then coordination during execution as adaptations to the plan are made. This sequence of events offers terrorists various opportunities to disrupt smooth operations of emergency responders. First, through various means, terrorists may attack, corrupt, or limit access to digitally encoded plans already in place for an emergency response but which must be consulted even by trained personnel. These plans may specify firefighting response procedures for specific buildings, cleanup procedures for chemical spills, and even organization flowcharts dictating how agencies will interact during a crisis.

A cyberattack targeted at these plans could take many different forms, from corrupting the plans so they are inconsistent or contradictory to denying access or even destroying the plans. Corrupting the plans might involve action by a trusted insider or the unauthorized access of an outside hacker, likely before the main attack. They might identify and replace the target plans with false ones. In this situation, emergency responders might follow procedures that they believe will help but really just increase the damage. This form of attack could take place at any point before the emergency. If the corruption remains undetected and unrepaired, it will have a detrimental effect on emergency operations. Another form of attack might employ a virus or denial-of-service attack on a database of plans to prevent access.

Next, we turn to execution of a response plan. As large-scale emergencies require action on the part of numerous individuals and agencies, terrorists may try to prevent the orders for execution from reaching some or all of the emergency response services. This could be accomplished mainly through attacking communication or computer systems. Communications disruptions are discussed in more detail below.

Military wisdom dictates that a good commander will plan extensively, and then modify the plan once on the battlefield. This idea also applies to emergency response. Once a crisis situation begins, it is important that emergency response managers adapt the original response plans as the situation requires. To maintain a disciplined response even when plans are adapted requires coordination throughout the entire response. In the Washington, D.C., emergency manage-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

ment plan, this is achieved by providing a central command and control activity in the EOC. By centralizing command and control, a high level of coordination is achieved even when plans change on short notice. However, communication between the EOC and the deployed responders is critical.

The centralized nature of the emergency command and control system makes it a prime target for terrorist disruption. Terrorists could shut down computer systems in the EOC using worms or other viruses or they could jam communications in and out of the center using denial-of-service attacks or other cyberattacks on the telecommunications systems. Another possibility is the use of an electromagnetic pulse (EMP) weapon against an EOC. This weapon is a portable device that delivers an electromagnetic pulse sufficiently strong to physically damage the operating condition of electronic systems such as computers, digital telephone switches, and other systems without necessarily causing permanent damage to the hardware.[4] If unshielded, an EMP device detonated within range of a city's EOC could effectively put it out of operation.

Emergency operations centers rely heavily on computers, which creates a number of vulnerabilities. Bugs and backdoors may exist in both the commercial software used (especially the Windows operating system) and the proprietary software developed specifically for emergency response coordination. Examples of this software include the Crisis Information Management System (CIMS), which the Washington, D.C., Emergency Management Agency uses. CIMS is a system for effectively sharing information among the various terminals in the EOC. With software increasingly being developed in foreign countries, there is an increased risk of bugs, exploits, and mistakes that terrorists could use being built into the software.

Finally, it is possible that the EOC could be damaged during a physical attack to the point of disrupting operations. This happened in the September 11, 2001, attack on New York City. The city's original emergency operations center was located in one of the World Trade Center towers and was destroyed when the towers collapsed. One of the main sources of vulnerability for emergency response is the highly centralized nature of its command and control apparatus. This gives terrorists one target that, if neutralized by cyberattacks, could greatly hinder the ability of emergency responders to implement an effective response to a physical attack.

INFORMED RESPONSES: ACCESS TO CRITICAL INFORMATION

Uncertainty characterizes emergency operations; the full situation on the ground may be unclear for some time. When emergency responders receive a

[4]Branscomb, L. M. 2004. Cyberattacks as an Amplifier in Terrorist Strategy. P. 95 in Terrorism—Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

call to respond to an emergency at a certain location, they usually only receive the most basic information about the nature and extent of the emergency. Emergency responders may not know what situation-specific information is needed until they are on site and have evaluated the crisis situation. This information must be obtained by the emergency responders not while they are at a central base of operations but while they are deployed. This may be especially true after a terrorist attack, in which full information about the attack would substantively impact the type of response required. In contrast to a natural disaster, terrorists may deliberately hide some of the elements of the emergency situation. For example, in a chemical attack, certainty about the exact chemical agent employed would allow responders to be safer and to be more effective and timely in their resource allocation. Future terrorist attacks could invoke combinations of different types of threatening situations.

As discussed in the section entitled "Critical Information," there is a wide range of information that could be critical in the response to a terrorist attack on an urban area. Responders in the field will need to call upon and receive various sorts of records, such as medical records to help correctly treat patients, building or city architectural and construction plans, or contamination and cleanup information on specific chemical or biological agents. Some of this information, such as individual medical records, needs to be current. It is not possible for the emergency responders to acquire all of the information ahead of time; instead, they need to access it from the definitive source. The necessity of this critical information about the specifics of the situation and the situation-specific response procedures opens up a variety of possible threats from cyberattacks that will disrupt the ability of responders to address an emergency situation.

Terrorists may attempt to corrupt critical information at its source using computer worms or entry by a trusted insider or hacker with unauthorized access. In this case, emergency responders would unwittingly acquire incorrect information. Medical records present a special challenge in this regard. Medical patient records should of necessity be available to doctors broadly and in near-real-time. The need for accessibility of this information and also its sheer volume make it a difficult target to secure against unauthorized entry. By breaking into these databases and, for example, changing the blood types or drug allergies of individuals, terrorists could cause incorrect blood or drugs to be administered to individuals in a crisis situation. Medical mistreatment may hurt the individual, but in addition, treatment errors may cause citizens to distrust the emergency responders. This increases the terror induced by attacks.

Another example is databases of contact information for emergency management officials. The D.C. Emergency Management Agency maintains databases of text messaging numbers and formats for emergency officials and databases of phone numbers of D.C. citizens. This information will be critical in quickly communicating with emergency officials and the public in a crisis. Un-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

authorized access by hackers or tampering by a trusted insider could falsify these databases so that communications are interrupted.

It is also possible to corrupt critical information that is not stored in centralized databases by emergency response agencies. For example, in any type of chemical or biological attack, emergency management officials will use information from remote meteorological sensors to create a computer plume model that will illustrate the spread of the chemical or biological agent based on wind patterns. Attacking the control programs of these sensors or corrupting the flow of information from the sensors to the EOC could seriously impair this effort. Even such a small change as replacing "east" with "west" in a wind report could have disastrous consequences for civilians.

Terrorists may attempt to limit the ability of responders to access this critical information while in the field. This may be achieved by limiting access to the applicable databases through a denial-of-service attack or by disrupting the communications of emergency managers or first responders. Denial-of-service attacks could bring down electronic mail servers and hacking or virus tactics could be used against cellular phone networks. As emergency responders begin to carry more portable computers with Internet access, attacks on Internet servers and databases could have an impact on the ability of first responders to access needed information.

ASSURED COMMUNICATION

Communication is the backbone of an emergency response. Effective, coordinated action requires communication between disparate groups and individuals. During an emergency response, communication flows in a number of different ways. Each of these channels or lines of communication can be potentially impacted or disrupted by a cyberattack. The first essential line of communication is from the public to the responder. This is the means by which the public will alert emergency services that an emergency exists and solicit aid. As discussed above, the 9-1-1 system is vulnerable to disruption in a variety of ways.

Beyond the 9-1-1 system there are other communication methods within this category that are also vulnerable to disruption. For example, many high-rise buildings have fire evacuation procedures that rely on disabled or trapped victims notifying rescuers of their location via an internal telephone system. Such a system, if not secured, might be vulnerable to attack. Likewise, in a widespread biological attack, citizens may need to call hotlines or hospitals to inform them of the spread of contagion.

The second main category of communication is within the emergency response apparatus. This category breaks down into a number of different forms of communication: communication within one autonomous emergency response agency (a fire department, for example), communication between emergency

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

response agencies or with the emergency management system, and communication between the emergency management system and nonlocal emergency organizations such as the Federal Emergency Management Agency (FEMA), the National Guard, and state and federal governments. Lastly, there is necessary communication from the government back to the citizens.

All of these different forms of communication are both vital and vulnerable to a cyberattack. Within one emergency response agency, communication will flow usually from a central dispatcher or management center to various units in the field. Within an organization the lines of communication are used in normal day-to-day operations, so they may not be strained as much during a large-scale emergency situation.

Communication between the various autonomous emergency response agencies and with the central emergency management agency is not used as frequently, and it is likely to be more vulnerable during a crisis. As noted in the section on preplanned and coordinated operations, communication between the different agencies on a macroscale will usually be coordinated by a central EOC. Disabling the computer and telecommunications systems of this center will impede communication. At the scene of the emergency, however, most communication will be face-to-face between the commanders of the different agencies responding to the situation. Although responders may coordinate their actions on the scene, their ability to call for additional resources may be impaired.

Because crisis situations strain communication bandwidth and range, emergency responders may turn to more ad hoc forms of communication. That is, they may use methods of communication that are not built into the system. For example, emergency responders and managers may use cellular phones and electronic mail to augment the existing communication. Both can be helpful in a crisis situation, but they are also vulnerable to disruption from a cyberattack. Cellular phones rely on towers and nodes to connect to the telephone network. These are vulnerable to a cyberattack that could disable cellular service across an urban area. Electronic mail can be disrupted by overloading the mail servers of the emergency response agencies through denial-of-service attacks or by shutting down these agency servers all together through the use of worms, viruses, or sabotage by trusted insiders or hackers.

Telephone, cellular phone, and electronic mail may also be the main way in which emergency responders and managers call upon regional and national resources to help in the emergency. In a large-scale emergency, urban area managers will need to effectively communicate with the regional, state, and federal governments. They may need to call upon the forces of the National Guard and the resources available through FEMA. Equally important, EOC officials will need the resources of business organizations that have their own communications networks, their own trucks, and possess a broad range of valuable expertise. Many of those businesses will be volunteering assistance. They will be using—or trying to use—conventional telecommunication methods such as the telephone and Internet. Dis-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

rupting telecommunications and electronic mail through the cybertactics discussed above could greatly impede this communication.

The necessity of integration with regional emergency services and agencies presents another facet to the security problem. Rapid communication with regional partners of an emergency management agency is necessary in a large-scale crisis situation. To ensure this, the communications systems have been designed in most cases to trust information coming from regional partners. This assumption of trust presents a situation where the security of an urban emergency management agency is only as good as the security of the weakest partner agency on which it relies. For example, the D.C. Emergency Management Agency works closely with the Virginia and Maryland emergency management groups and various emergency response units in neighboring jurisdictions. An attack on any of these regional partner agencies could be used to spread misinformation. Misinformation planted at a regional partner agency will be considered trustworthy by the urban emergency management agency. This is a real problem, as many county and local emergency response units do not have the resources to implement the computer security that urban emergency response groups may have.

The final vital form of communication is from the emergency response system of agencies to the general public. Emergency responders need to inform victims of the emergency what their course of action should be. In addition, those who are not directly a victim of the attack need to know that the government is taking action to alleviate the situation or they might lose faith in the ability of the government to protect them. This communication will mostly take place through television and radio. It is unlikely that this communication could be substantively disrupted because of the many alternative media channels and the existence of the preplanned emergency radio broadcast network (in the United States).

Increasingly, government agencies post information on web sites and send electronic mail directly. The D.C. Emergency Management Agency maintains an EOC web site with which it communicates both with the public and with emergency services of surrounding areas. Terrorists may attack the computer systems that operate television and radio stations. They might prevent the government from making use of some of these media outlets or they might plant false broadcasts that will increase public terror. Web sites where information is posted are easy targets to attack. Denial-of-service attacks could be used to disrupt access to a particular site or hackers could gain unauthorized access to the site and plant false messages.

There are numerous examples of hackers defacing web sites for political goals. Pakistani hackers have in the past gained unauthorized access to the web sites of the Indian Parliament and India's Department of Atomic Energy, stealing information and defacing the web sites. In the Israeli-Palestinian conflict, statistics show that politically tumultuous events have caused increases in the

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

defacement and disruption of Israeli computer systems by hackers. Finally, after the April 2001 midair collision of a U.S. surveillance plane and Chinese fighter plane, Chinese hacker groups organized and sustained a week-long cybercampaign against U.S. targets. They used denial-of-service attacks to limit the operability of U.S. systems and inserted pro-Chinese images into many U.S. government web sites.[5] It is possible that hackers could gain access to web sites on which the government would post emergency information and replace it with incorrect information for the public to access.

In summary, communication during a crisis situation will be a critical part of the emergency response. Coordination is required for an effective response, and rapid, secure communication is the only way to conduct such coordination. A large-scale emergency will stress the communication between organizations that are normally autonomous and in some cases competitive. The necessity of communication and the stress on the system make the lines of communication an attractive target for terrorists hoping to disrupt an emergency response and amplify the effects of a physical attack.

CONCLUSION

Cyberterrorism is often dismissed as an unlikely tactic of serious terrorist organizations because its results are seen mainly as a nuisance and unlikely to produce casualties. It is clear, however, that a well-thought-out cyberattack on emergency responders could significantly amplify the damage resulting from a physical attack. This paper has attempted to identify the salient properties of an emergency response effort, and then examine a few ways in which the emergency response might be impeded by cyberattacks. Not only must individual agencies work on protecting themselves from cyberattack during a crisis, they must be able to mount a coherent cyberdefense under the stress of a crisis.

Our working group believes that Russia and the United States share this problem. The governments in both countries need to think through how to avert cyberattacks directed at emergency response activities. Policies, plans, and budgets need to be put in place to assure the functioning of emergency responders.

[5]Vatis, M. 2001. Cyber Attacks During the War on Terrorism: A Predictive Analysis. Hanover, NH: Institute for Security Technology Studies at Dartmouth College, September 22, 2001. See pp. 7–11 of http://www.ists.dartmouth.edu/lib_assessments2.php.

Copyright National Academy of Sciences. All rights reserved.

News and Terrorism: Communicating in a Crisis

Randy Atkins
Media Relations, National Academy of Engineering

THE NEWS MEDIA AS A CRITICAL INFRASTRUCTURE

Since the terrorist attacks of September 11, 2001, the U.S. government has repeatedly warned its citizens that a similar (or even more deadly) attack within its borders is not a matter of if, but when. Far-reaching efforts have been made to prevent and prepare for such a crisis. Officials are working to harden every conceivable critical infrastructure target, but at first, one was overlooked: the news media.

Maybe that is because few people think of the news media as a part of their nation's critical infrastructure, and in the United States, it is (thankfully) outside government regulation. When we think of infrastructure, we usually think of tangible things like energy pipelines, transportation systems, and computer networks. With the advent of modern terrorism, the news media also belong in this category. They are the main communication conduit to any nation's most important infrastructure: its citizens.

While the connectedness of modern infrastructures means greater efficiency, it also creates new types of interdependencies that expose new vulnerabilities. The news media may in fact be the weakest link in the system. We need to protect the media as zealously as we protect the electric power grid and nuclear reactors, and not just their printing plants and broadcast towers.

The agencies and officials working to bolster homeland defense need to work more closely with journalists and with organizations like the U.S. National Academies. Journalists need to be armed with the knowledge to work effectively as part of the nation's response to terrorism. To do that, they need the help of the engineering, science, and medical communities.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

At the National Academy of Engineering (NAE), we wrestled with the question of how to help the media become better informed and more conscious of their importance during a terrorist attack. Journalists in the United States are constitutionally protected and vigorously independent. No one can dictate what stories they choose or how they are reported.

Many in the U.S. government (probably in all governments) think of journalists as pests, even as threats to national security. The feeling is often that reporters should be avoided as much as possible and told as little as possible. Especially in current times, the opposite is true.

A study by the New York Academy of Medicine[1] says that "far fewer people than needed would follow protective instructions" during terrorist attacks involving smallpox or a radiological bomb. People will not blindly do as the government tells them; they need to understand the reasons for actions being taken. In the midst of a terrorist attack involving weapons of mass destruction, effectively communicating potentially complex information will be a difficult challenge that will fall largely upon the news media.

Getting good information to the public in the midst of a crisis can actually be more vital than the actions of first responders. In fact, journalists *are* first responders. Not only do they sometimes arrive at the scene first but they are the only ones focused on and able to communicate risk to people in real time. They can save lives through efficient delivery of accurate information.

Yet, with today's competitive 24-hour news coverage, journalists are under tremendous pressure to fill airtime and print space and to get the story first. Of course, this can lead to speculation, and it is not always harmless. Sometimes it can cost lives. This is not just the media's problem; it is not just the government's problem. It is the engineering and science communities' problem, too.

The NAE decided to conduct a tabletop terrorism scenario exercise that would, for the first time, focus on communication issues. The goals would include simply bringing together groups that do not often work together—journalists, scientists, government officials—to meet and begin to understand each other's needs during the chaos of a terrorist attack. Situations can look much different when viewed from another perspective, and the time to start a relationship is not during a crisis.

Government officials must understand the pressures journalists face when trying to report relevant information under the pressure of continuous coverage during a crisis. Journalists, in turn, must better realize the need of government spokespeople to be cautious. Scientists should be prepared to deviate from their ultraprecise tendencies and convey their expertise in ways that laypeople understand.

---

[1]Lasker, R. D. 2004. Redefining Readiness: Terrorism Planning Through the Eyes of the Public. New York: The New York Academy of Medicine.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Journalists, in particular, have few precedents for this new type of warfare—it is different from traditional war reporting. They need a strategy to deal with it and an instant pool of trusted experts who are good communicators.

On June 20, 2003, the National Academies hosted, in association with the Greater Washington, D.C., Board of Trade and the U.S. Department of Homeland Security (DHS), a terrorism scenario simulation, entitled Media and the First Response, which engaged all of the above groups.[2] The event was so successful that the DHS provided funding for the National Academies to conduct similar workshops in 10 cities across the United States.[3] The National Academies worked closely with both DHS and the Radio-Television News Directors Foundation (RTNDF) to create this series, called News and Terrorism: Communicating in a Crisis.

HELPING THE PIECES WORK TOGETHER

The nationwide News and Terrorism: Communicating in a Crisis workshops began in August 2004. Approximately 100 invitees attend in each city, mainly journalists; government officials; science, engineering, and medical experts; and emergency responders. The workshops include a background presentation on the science and technology behind potential terrorism threats and information on self-protection when near various terrorist incidents. The centerpiece is an exercise in which seven to eight people (journalists, government officials, and a technical expert) react to an unfolding terrorism scenario.

Scenario simulations are powerful tools for vividly illustrating problems and uncovering system weaknesses. Commonly used by the military for many years, such exercises are being used more and more frequently by emergency officials and even private industries.

It is difficult to prepare for events that have not happened before. Thinking through the communication flow in a crisis, before it actually occurs, is vital in this information age. The public expects to be informed right away, and they will be. The main questions are: by whom, and how well?

Examples of dialog from our scenario exercises cannot be shared, because the ground rules require that the comments of participants not be for attribution in any public forum. This allows the players in our war games to be open and honest, knowing that their candid remarks will not appear in the newspaper the next day. While much of the dialog might actually increase public confidence in the preparedness of those tasked with keeping us informed, too much of it would certainly cause unease.

[2]See http://www.nae.edu/nae/naehome.nsf/weblinks/CGOZ-5NWKDB?OpenDocument.
[3]See http://www.nae.edu/NAE/naehome.nsf/weblinks/CGOZ-642NPX?OpenDocument.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

A demonstration of the kind of interactions revealed during these workshops need not come from the exercises themselves, however. Real life provides very good examples.

On September 30, 2001, U.S. Health and Human Services Secretary Tommy Thompson appeared on the CBS television network program *60 Minutes* and said, "We're prepared to take care of any contingency, any consequence that develops for any kind of bioterrorism attack." He did not know that such an attack was already under way, and his remarks would soon be severely tested.

On October 4, 2001, Florida officials announced that tabloid magazine editor Bob Stevens had been diagnosed with inhalation anthrax. Later that day, Secretary Thompson made a rare appearance at a White House press briefing. He was joined by an expert in biological threats, Dr. Scott Lillibridge.

After making a brief statement about the situation involving Mr. Stevens, Secretary Thompson was peppered with questions from journalists. The second one asked whether Mr. Stevens had come in contact with raw wool or if he might be a gardener, to which Secretary Thompson responded:[4]

> *SECRETARY THOMPSON:* We have the FBI [Federal Bureau of Investigation] and we have dispatched, . . . as soon as we heard anything suspicious, we have our CDC [Centers for Disease Control and Prevention] officials there, on the ground. And they are going to go through—the last couple weeks, go to the restaurants. He traveled to North Carolina. We've also dispatched people from CDC to North Carolina, to the communities that he was there. We're checking with his neighbors. We're investigating with the FBI all known places and all the things that he might have ingested.
> *JOURNALIST:* Mr. Secretary, what are some of the sources that could cause such an infection?
> *SECRETARY THOMPSON:* That's why the doctor is here. And do you want to answer that?
> *DR. LILLIBRIDGE:* Sure. Sporadic cases may occur from contact with wool, animal products, hides, that sort of thing. And occasionally we don't know the context of these. These are sporadic, episodic things that happen from time to time.
> *JOURNALIST:* But how sporadic? You just named two cases last year in Texas and then Florida in 1974. That's two . . .
> *SECRETARY THOMPSON:* They're very rare. It's very rare.
> *JOURNALIST:* So this is the third since 1974?
> *SECRETARY THOMPSON:* We don't know that, but this is a confirmed, and at this point in time, it's an isolated case. And there is no other indications anybody else has got anthrax.

[4]Thompson, T., and S. Lillibridge. 2001. White House Press Briefing, Washington, D.C., October 4. See http://www.whitehouse.gov/news/releases/2001/10/20011004-12.html.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

JOURNALIST: Do you know if he happened to work around wool or any of the products that might have . . .
SECRETARY THOMPSON: We don't know that at this point in time. That's entirely possible. We do know that he drank water out of a stream when he was traveling to North Carolina last week . . .

Biological disease expert Dr. Lillibridge continued to be ignored during the next 13 questions, though many of them involved technical issues and questions about symptoms. Finally, Secretary Thompson turned to Dr. Lillibridge when a questioner probed about how likely it was that there had been other anthrax cases in the past year that had gone undiagnosed.

SECRETARY THOMPSON: It's entirely possible.
JOURNALIST: Possible or likely or. . . ?
SECRETARY THOMPSON: Would you say it's probable?
DR. LILLIBRIDGE: It's possible. As you heighten surveillance, you'll get more.

That response was the last heard from Dr. Lillibridge. The news media seemed more interested in getting a good quote from a high-profile cabinet secretary than in understanding what they need to report to the U.S. public.

It did not help that Secretary Thompson was trying his best to dismiss the possibility of terrorism while making statements uninformed by science. Either he should have been better briefed on the facts, or he was shading the truth. Either way, the public was not served well.

There were five more questions, all directed at Secretary Thompson, before White House Press Secretary Ari Fleischer wrapped up the subject of anthrax and turned the press conference to other matters, saying: "Any additional information will be made available by either the CDC or the HHS [U.S. Department of Health and Human Services]."

The White House obviously commands center stage in the middle of such crises. Are they equipped to effectively communicate the science and risks? These sorts of issues are dramatically brought to light, just as in this example, through our mock scenarios.

In the real-life case, as Mr. Fleischer tried to move on to another subject, the journalists' questions continued, asking for verification of Dr. Lillibridge's name and then following up by asking: "Is he an M.D. or a Ph.D?" Mr. Fleischer responded, "I'd have to look that up. I couldn't tell you. You may want to just check with HHS."

The scientist, who is best equipped to inform the public about potential dangers or lack thereof, was not even important enough for a White House follow-up. The journalists, too, missed many opportunities to get solid facts from him. These are lessons that should have been learned in postanalysis of the 2001 anthrax attacks, but that is not yet evident. Similar mistakes during our scenario-based workshops are sometimes frightening. Hopefully those in attendance are now doing something about it.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Let us return to the real-life events. On October 15, 2001, less than two weeks after the Stevens diagnosis and just a few days after it was announced that an NBC News employee in New York had also been infected with anthrax, an intern in U.S. Senator Thomas Daschle's office opened an envelope containing white powder that tests confirm contained anthrax. The next day, Senator Daschle stepped before the media's microphones and began talking about a foreign operations bill. Of course, the first question from journalists was about anthrax:[5]

> *JOURNALIST:* Senator, there are a dozen Senate offices closed today. There is no mail. People are being tested for anthrax. How is the Senate functioning?
> *SENATOR DASCHLE:* I think the Senate is functioning as we could hope it would. Obviously, these are difficult times, and we are going to have logistic and administrative challenges that we're going to have to face. But I think understand [*sic*] the circumstances, the Senate is functioning quite well. We'll be back in business in all respects within the next several days.

Although Senator Daschle lacks scientific expertise, the journalists went on to question him about technical issues:

> *JOURNALIST:* If today it was so important to close the Hart Building partially as a precaution, why wasn't it important to do that yesterday? And do you think that people might have been put at risk by that?
> *SENATOR DASCHLE:* I am confident that there was really no risk involved. This was simply an effort to determine whether there is even a modicum of anthrax that could be found in one of the vents or one of the air ducts that would give us some indication that there was dissemination. Keep in mind that even if there is some trace, it wouldn't be of sufficient force or strength to be of health risk to those who are exposed.

Should Senator Daschle be the spokesperson to the American public about such issues? Does he have scientific credibility? The next day, leaders of the U.S. House of Representatives held a widely broadcast news conference in which they, too, were asked about the technical nature of the anthrax.[6]

> *JOURNALIST:* Who briefed you on the anthrax? Who told you that it was sophisticated? Because the senators are now saying that it was garden variety anthrax.
> *CONGRESSMAN [J. DENNIS] HASTERT:* You know, we're just saying that the way that it was distributed, with a flume, was unlike anything that we've seen up to this point. Of course, we weren't in contact or saw what happened in

[5]FDCH Political Transcripts. 2001. U.S. Senator Thomas Daschle (D-SD) holds news conference. October 16.

[6]FDCH Political Transcripts. 2001. Representatives Hastert and Gephardt hold news conference. October 17.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

> the building in Florida or any of those buildings in New York. But this was different from the anthrax that was just out there in an envelope on a white, powdery substance. It actually had a flume and, you know, infected a lot of people.
> *JOURNALIST:* Is there something that propelled it?
> *CONGRESSMAN [RICHARD] GEPHARDT:* No, it was the same as the other situations. But you had now 29 or 30 people who have tested positive. That's a new development. Obviously, that's more than we've seen in these other instances. And it led the people who have looked at this to believe that it is a higher grade, weapon-grade kind of anthrax.

Journalists too often turn toward congressional people and other high-profile celebrities with little expertise in the science at the heart of issues involving potential weapons of mass destruction. In this case, conflicting statements between public officials certainly did not reassure the public. Why were members of Congress the lead spokespeople in the midst of such a technologically complex situation? Why were not those at the forefront of the issue scientists with expertise in anthrax bacteria or airflow physics, engineers who could discuss ventilation systems, and medical professionals who could talk about patient symptoms?

Our News and Terrorism workshops are designed to help such issues bubble to the surface and create a discussion among key players about how to do it better in real life. We have also produced four-page fact sheets on radiological, chemical, biological, and nuclear threats.[7] The purpose is mainly to help journalists (though others would find them useful, too) become knowledgeable enough not only to report accurate information to the public but also to simply ask the right questions.

EFFECTIVELY SERVING THE PUBLIC

Most journalists are not engaged enough on the underlying issues, the substance and context behind breaking news, which often involve science and technology. So their questions are at a superficial level. The News and Terrorism scenarios are a dynamic way of pulling people into important discussions. Getting the interest of journalists when there is not an immediate threat is a challenge, but a vitally important one.

Too often the news media takes the easiest path, which often means the political angle. In part, this is because politics is a form of theater, and entertainment trumps substance in the economically driven media. Politics is also about people and personalities. The news audience, unfortunately, has been trained to have a limited and shallow attention span.

[7]See http://www.nae.edu/NAE/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

If journalists are going to report in sensational and inaccurate ways, then some might argue that journalists should simply be barred from reporting about terrorist incidents. That way, the terrorists would not have a stage. But fear of the unknown fuels terror too, and distrust in government stems from such withholding of information. People will get their news, if not from the media, then through the rumor mill. When it works correctly, independent professional journalism is the best way to inform the public. That is why the First Amendment of the U.S. Constitution[8] is so important.

We need the media not only to become a stronger part of our infrastructure but to keep challenging the government, because that exercise makes us all stronger. However, uninformed journalists cannot effectively question authority. For example, some well-meaning government efforts to classify or withhold information could end up actually harming national security by slowing the delivery of scientific research results beneficial to society. Journalists need to be equipped to effectively question such policies, and even the work of scientists. To that end, we should help journalists become better informed.

Even without direct government interference in news reporting, new technologies are now cutting out the journalistic middleman. For example, officials can send emergency instructions directly to personal devices like cellular phones (through which person-to-person reporting, including rumors, would also be conveyed). The public should not rely on such sources alone. Unless people are well informed, through independent professional sources, they will not know how to analyze the issues and how to assess the information being provided by their leaders.

The public will not automatically follow orders from authorities. Citizens need to understand the reasons for actions they are being asked to take, and they can deal with bad news. Those who seek to calm for the sole sake of maintaining order will ultimately create the opposite effect, and the public will begin to lose trust in its government. This is the ultimate goal of terrorists.

The public must understand the truth about real dangers. People will respond well, if the conveyor of information is perceived as trustworthy. Unfortunately, right now neither the government nor journalists are held in very high regard. We must work to change that.

Firefighters, police, and government officials are not always (maybe not even usually) the most important first responders. Often that role falls on such citizens as school teachers or even the media. They all need to understand, and can handle, the truth. Authority figures should not have an information mo-

[8]"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." The Constitution of the United States. Amendment I.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

nopoly. The more people are empowered to respond appropriately, the more secure we all will be.

As a local police chief once said: "You can't build a fence around a community, but you can arm your citizens with knowledge." Scientists, engineers, and the government must work to get good information into the hands of the media quickly during a cyber-, radiological, nuclear, chemical, or biological attack. We must all work together to determine the best way of doing that.

It is at our own risk that the technical community thinks of its homeland security responsibility as simply creating the latest counterterrorism technologies. They should also help empower the media, and thus the public, with knowledge. Ignorance and misinformation can be as damaging to the information infrastructure of a nation as a break in an oil pipeline. It can cause paralysis among citizens who are often the best first responders, confuse professionals trying to respond to a crisis, and help generate the fear that is the terrorists' goal.

Copyright National Academy of Sciences. All rights reserved.

Problems of Urban Terrorism in Russia

Konstantin V. Frolov
Mechanical Engineering Research Institute of the
Russian Academy of Sciences

Today in Russia and in the world, problems of protecting the population, critically important infrastructure elements, and the environment against natural and technogenic disasters and terrorist attacks have become some of our most significant priorities. Under the leadership of the president of the Russian Federation, the Security Council and the Presidium of the State Council discussed these problems at a meeting on November 13, 2003, and passed a number of important resolutions. As a result, for the first time in our country at such a high and prestigious level, the Russian Academy of Sciences, the Ministry of Emergency Situations, and the Ministry of Science and Industry were authorized to develop a Program of Basic Research and Applied Analysis on these problems for 2004–2010. This program includes instructions and major objectives for scientific development in the area of sociopolitical, economic, national, and regional sources of terrorism-related threats; principles for analyzing and monitoring the consequences of crises and disasters caused by terrorism; and consideration of terrorism in the overall strategic risks faced by the country.

The most important special feature of urban terrorism in Russia, as in other countries, is the abrupt increase in direct damage (loss of life, destruction of infrastructure) and indirect negative impact (fear, panic, paralysis of control) caused by the high concentration of population, potentially dangerous objects, and increased opportunities for maintaining secrecy and preparing terrorist attacks.

The most vulnerable targets for terrorist activities are Russia's major cities—Moscow, first of all, as well as the large cities and towns in areas marked by social and political instability and military conflict (Grozny, Makhachkala,

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Vladikavkaz, Nazran, Beslan). These cities are the focus of 90–95 percent of terrorist attacks.

Following is a breakdown of targets of urban terrorism:[1]

- Eighty-five to ninety percent of the targets are public transportation systems (metro, buses, trains, airplanes) and military transportation systems (automobiles, armored personnel carriers, tanks, helicopters).
- Three to five percent are mass gatherings of people (markets, theaters, stadiums, shops).
- Two to four percent are gas and oil pipelines in urban zones.
- One to three percent are power supply lines and transformer electrical stations.

Russia faces extraordinary danger in view of the considerable increase (by three to five times) in the quantity and gravity of terrorist attacks in comparison with the increase in the quantity and impact of natural and technogenic disasters. In this sense, the year 2004 was most significant, given the tragedies in Beslan and Moscow and on civilian aircraft, which involved the loss of hundreds of people, including children.

These terrorism trends in Russia have led to the need to implement comprehensive organizational, programmatic, scientific, and social measures, which will be described in more detail later in this meeting by our Russian experts. This paper mentions a few measures in which the Russian Academy of Sciences and the special working group under the president of the Russian Academy of Sciences provided leadership and supervision:

- meeting of the Interdisciplinary Committee on Disasters, at which the Report of the Russian Academy of Sciences on Problems of Technological Terrorism was presented (2000)
- Scientific and Industrial Conference on Technological Terrorism and Terrorist Threat Prevention Methods (2003)
- meetings of the Working Group on Risk Analysis and Safety Problems of the President of the Russian Academy of Sciences, including discussion of general and special questions of terrorism prevention (tagging of explosive materials, controlled detonators, creation of protection systems) (2001–2004)
- International Conference on the Safety of Large Cities (2003)
- special seminar within the framework of the Committee on Scientific and

[1]This breakdown covers the period from 1998 to 2002. See Russian Academy of Sciences, Russian Ministry of Emergency Situations. 2004. P. 313 in Problems of Technological Terrorism and Methods of Countering Terrorist Threats: Compilation of Materials from a Scientific and Practical Conference. Moscow: Institute of Mechanical Engineering of the Russian Academy of Sciences.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Technological Cooperation between Russia and the North Atlantic Treaty Organization (NATO) (2004)

- publication of special monographs, conference proceedings, and the series *Russia's Security* on interdisciplinary aspects of terrorism

During recent years, the scientists of the Russian Academy of Sciences and other Russian scientific organizations have carried out important work under the state scientific and technical program on security, as have Moscow researchers under the comprehensive program on Moscow's security. One major result of this work has been the development and approval of the Security Principles for Moscow in 2000 by the Moscow city government. This document represents the officially adopted system of views on the objectives, tasks, basic principles, and directions of activities for ensuring the security and sustainable development of the city under conditions of possible external and internal dangers and threats. These principles are approved as the basis for the following:

- development of security strategy
- improvement and further development of the legal and regulatory base for the provision of security
- development and implementation of special programs for providing security against specific threats
- formation and implementation of joint policy by the city administration, economic and social entities, and the city's population with the aim of ensuring the security of Moscow

The Security Principles for Moscow include the following types of threats: social, political, terrorist, natural, technogenic, environmental, informational, psychological, criminal, and military. At present in Moscow, priorities have been set for development program implementation strategy and corresponding program activities. Chief among them is the improvement of the effectiveness of measures to counteract terrorist activities.

The Security Principles of Moscow provide the following description of terrorist threats:

> Terrorism has become one of the most dangerous challenges for the security of society. It poses a special hazard for large cities and political, economic, and cultural centers. Acts of terrorism have been increasing in scale and becoming more multifaceted from the standpoint of objects targeted and method of implementation. Terrorism has the opportunity to use the achievements of science and technology for its criminal pursuits.

The main threats from terrorism are as follows:

- attacks on political and economic entities (seizure, bombing, arson, and so forth)

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- bombings and other terrorist acts in crowded areas (metro, railway stations and terminals, means of transportation, residential areas)
- kidnappings and seizures of hostages
- hijackings of airplanes and other means of public transportation
- attacks on facilities that are potential threats to the population in an effort to destroy them or disrupt technological operations
- disruption of aviation and rail traffic control systems, power supply lines, means of communications, computers, and other electronic devices (electromagnetic terrorism)
- disruption of the psychophysical state of the population by means of programming behavior or activities of large population groups
- cyberattacks against the most important computer networks
- dissemination of information in the press and on radio and television that may distort public opinion and cause civil commotion
- disruption of information networks
- dispersion of chemical and radioactive materials in crowded areas
- contamination of water supply systems and foods
- dispersion of infectious pathogenic organisms

The main preconditions aggravating the rise of terrorist threats are as follows:

- combination of organized terrorist groups with a large quantity of independent, autonomous cells and individuals
- appearance of new kinds of terrorism (informational, technogenic,[2] cybernetic)
- expansion of the means of terrorist activity (biological, chemical, radiological, and so forth)
- absence of motivation and unpredictability of so-called unscrupulous terrorism, in which violence is aimed at the disorderly murder of certain individuals
- increase in the intellectual level of terrorism relative to the pace of development of science and technology

Realization of the above-mentioned threats may cause

- disruption of the public order in the city for long periods of time
- creation of a climate of fear
- large numbers of casualties

[2]Technogenic, or technological terrorism is represented by actions aimed against infrastructure targets critical to national security or committed using especially dangerous technologies, devices, and materials. Konstantin Frolov, e-mail message, March 15, 2006.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

In accordance with the Security Principles of Moscow, the main measures to ensure the security of the city in terms of preventing, detecting, and suppressing terrorist activity and minimizing its consequences are as follows:

- identification and elimination of causes and conditions that may support further terrorist activities
- ideological, informational, administrative, and organizational efforts to counter and prevent the formation of terrorist intentions in people's minds
- legal, informational, and administrative efforts to counteract the rise of terrorist groups and organizations
- institution of a ban on importing terrorist means (ammunition, explosives, dangerous chemical agents, and so forth) into the city
- creation of a city system for the efficient suppression of terrorist actions
- implementation of a set of special measures to protect especially dangerous facilities and sites
- creation of a crisis management system covering the period from the initial threat of a terrorist act through the elimination of its consequences
- organization of effective cooperation between all federal and municipal structures involved in counterterrorism activities
- improvement of the technical means used for eliminating the consequences of terrorist acts
- upgrading of monitoring systems for detecting radioactive and chemical materials and biological agents
- formation of specialized municipal chemical and biological emergency response groups
- heightening of industrial safety to reduce the risks of technogenic terrorism

Pursuit of objectives aimed at ensuring the city's security and development and implementation of measures for their fulfillment must be carried out in accordance with the following main principles:

- The principle of general obligation ensures the security of the city by making it the obligatory function of all federal government agencies, local government institutions, enterprises, organizations, companies, and various legal and organizational entities as well as the obligation of every citizen.
- The principle of legal dependence ensures the security of the city is carried out in strict accordance with the Constitution of the Russian Federation, current Russian Federation legislation, the Principles of the National Security of the Russian Federation, the Moscow city charter, and Moscow city legislation.
- The principle of universality assures that measures to ensure the security of the city are organized and carried out with regard to the potential realization of any reasonably probable kind of threat.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- The principle of prevention assures that measures to ensure the security of the city are organized first and foremost in the interests of threat prevention and carried out in advance in conjunction with the efficient increase in their volume and intensity.
- The principle of reasonable sufficiency assures that measures to ensure the security of the city are planned and carried out with an eye to the reasonable adequacy of their volume, duration, and economic basis.
- The principle of differentiation assures that the nature, volume, duration, and order of implementation of measures to ensure the security of the city corresponds to the special characteristics of each administrative region and city district, enterprise, organization, and company and guarantee the rational use of labor, material resources, and funds.
- The principle of coordinated control ensures the security of the city based on a division of responsibilities between federal government entities, local government institutions, and the administrations of enterprises, organizations, and companies. It is based on a combination of centralism in control over the measures and obligatory active control for their implementation in all entities.

We hope that the results of our work in Washington, D.C., and New York City and our practical recommendations will be used in Russia and Moscow in implementing and further developing the principles that have been adopted for reducing the risks of terrorism.

Copyright National Academy of Sciences. All rights reserved.

Terrorist Acts in Moscow: Experience and Lessons in Eliminating Their Consequences

Aleksandr Yu. Kudrin
Main Administration for the City of Moscow of the
Russian Ministry of Emergency Situations;
Center for Monitoring and Forecasting of Emergency Situations

Moscow is the capital of the Russian state and the spiritual center of the Russian land. It is the center of the scientific and cultural life of the country, with a significant portion of the national wealth concentrated within its territory. It is a unique historical and architectural monument of world culture. It represents the largest concentration of financial and information flows and has a substantial influence on the development of the state. It is Russia's largest industrial city, making a significant contribution to the country's overall economic indicators. Moscow has the country's most developed energy and public utility networks. Our city is the country's most important transportation hub, on which the functioning of the entire Russian transportation system depends.

Furthermore, unique tall buildings are being constructed and put into service in the city, and new metro stations are being built along with underground shopping and entertainment centers, tunnels, and parking garages. Thousands of industrial enterprises are located in the city. Disruption of their normal operations, and especially terrorist acts and accidents at their facilities, could present a significant danger to every resident.

Despite the measures being undertaken, Muscovites have been confronted with inhumane and antihuman manifestations of terrorism in recent years. Therefore, we understand and share the pain and suffering of other peoples that have suffered from extreme situations of any nature. We recall the seizure of hostages during the theatrical show *Nord-Ost,* as well as the bombings at the shopping center in Manezh Square; in the underground pedestrian passage at the Pushkinskaya Metro Station; outside the National Hotel and the Rizhskaya Metro Station; during the concert at the Tushino Airfield; and in a metro train car in the

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Paveletskaya Station, all of which resulted in more than 3,000 victims, about 700 of whom were killed.

These events demonstrated that terrorist acts are increasingly moving from the realm of potential threats into that of actual extreme situations. In our opinion it was the lack of the appropriate reaction from the world community to the fall 1999 terrorist acts in Moscow that led to the tragic events of September 11, 2001, in the United States, events that once again showed that terrorism has no nationality, that it is international in nature, and that no state is insured against it.

RESPONSE AND ELIMINATION OF CONSEQUENCES

In addition, accidents at facilities that use dangerous chemical substances in their production processes represent another serious potential danger for the city. Indeed, accidents at such facilities could lead to the chemical contamination of large sections of the city.

For example, on April 26, 2004, an accident involving the release of ammonia into the atmosphere occurred at one of the city's dangerous facilities. Subsequently analyzing the causes of the accident, one may conclude that it occurred due to the most egregious violations of the rules of technological safety. In the interests of obtaining the greatest possible profits, the management of the enterprise neglected to carry out mandated work and maintenance on systems and utility lines at the facility. An explosion resulted, and the production facilities were destroyed. Only the wise actions of the city's response services and favorable meteorological conditions prevented the contamination cloud from spreading over neighboring enterprises and residential blocks.

In contrast, our greatest efforts were required to eliminate the consequences of the bombings of the apartment buildings on Guryanov Street (September 9, 1999) and Kashirskoe Shosse (September 13, 1999) and to extinguish the fire in the Ostankino television tower (August 27, 2000).

Using these examples, I would like to explain the organization of the system of efforts to eliminate the consequences of extreme situations.

From the moment that the first search-and-rescue units and fire crews arrived on the scene, the Main Operational Headquarters for Eliminating the Consequences of Emergency Situations in the City of Moscow deployed its personnel and organized cooperation with the local authorities, the Moscow City Commission on Eliminating the Consequences of Emergency Situations, the city emergency services, the Russian Ministry of Emergency Situations, and other federal agencies. Thus, a two-level management system has been organized and has proven its effectiveness.

Fire crews and search-and-rescue units from the Moscow Main Administration for Civil Defense and Emergency Situations, personnel and resources from the Russian Ministry of Emergency Situations, and the city emergency services were directly deployed for rescue operations. This created a group including a

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

total of more than 1,000 persons and 200 pieces of equipment. Efforts were organized in shifts.

In extinguishing the fire at the Ostankino television tower, we encountered the need to apply new tactics in conducting rescue operations. When the fire broke out on the fifth floor of the television transmitter section (400 meters aboveground) of the television tower (which has a total height of 540 meters), preliminary information indicated that the fire occurred as a result of a short circuit in vertical cable lines in a room housing receiving-transmitting feeder devices. Based on the results of an analysis conducted by investigators, tactics were worked out and the optimal personnel and equipment were selected to carry out search-and-rescue operations and extinguish the fire at the focus of this emergency situation. The following objectives were established:

- cutting cables
- covering the interiors of the cable shafts with sheets of damp asbestos to prevent the fire from spreading
- organizing a search for the elevator on which the cables had been severed within the tower
- ensuring security for personnel and removing some of them to a zone at a safe distance
- involving specialists from the Moscow City Trust for Geologic, Geodesic, and Cartographic Work to maintain constant watch over any deviations of the tower from the vertical axis

RESCUE EFFORTS

The experience gained in eliminating the consequences of these emergency situations has shown that the most serious attention must be devoted to matters regarding the management and comprehensive execution of rescue efforts.

In conducting these efforts, the personnel involved were provided with continuous, 24-hour meal service at two mobile food distribution points and one cafeteria. During the emergency situation, about 30,000 hot meals and cold sandwich meals were served.

A system was also established for refueling all equipment and vehicles involved. More than 7.5 metric tons of fuel, oil, and lubricants were used. The emergency response group was also provided with the necessary expendable supplies and tools.

The personnel involved in the emergency situation were able to warm themselves in special inflatable modules and buses.

Heavy equipment, including cranes, loaders, and dump trucks to remove structural debris, was put into action from the very first hours of the emergency situation. This equipment arrived from facilities located around the city of Moscow. Experience amassed in cleanup efforts after building demolitions has shown

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

that in such major emergency situations it is most expedient and efficient to use heavy cranes with a load capacity of 50 metric tons and a 20–40 meter swing-away jib. Cranes with a load capacity of up to 300 metric tons were subsequently used to bring down structures in danger of collapse.

Medical support was organized in accordance with the action plan of the Moscow City Center for Urgent Medical Care in Emergency Situations. Victims were sent to 13 different treatment facilities in the city.

Ambulance brigades were put in place around the perimeter of the emergency zone to provide medical care on site and take the injured to city hospitals. The entire effort involved 80 ambulance brigades and 3 brigades for the transportation of the dead (the bodies were delivered to official morgues on orders from a representative of the city Medical Examiner's Office).

A group of psychologists was organized to work in hospitals and clinics and a hotline was established for relatives of the victims.

Because operations went on 24 hours a day, we had to resolve questions regarding how to illuminate the work area during the hours of darkness. During the first hours (which occurred at night), the area in which rescue efforts were being carried out was lit by individual lighting devices belonging to the search-and-rescue units of the Moscow Main Administration for Civil Defense and Emergency Situations. Lighting was subsequently organized by a special unit of the Moscow city government, which set up powerful lighting equipment. The efforts organized and undertaken made it possible to ensure that there was sufficient light in the areas where work was under way.

Experience shows that success in carrying out rescue efforts largely depends on how the efforts are organized in the initial hours. The primary organizational task in this regard is determining the most important areas in which to focus the work, the number of people and pieces of equipment needed at the given stage, and their placement around the site. It is also important to register personnel and equipment upon their arrival and establish a shift schedule for people and equipment over the course of the operation.

SECURITY AND PREVENTION

It must be noted that ensuring security against emergency situations and terrorist acts is a complex and multifaceted problem, and its successful solution may be achieved only through the active participation of all city structures, federal ministries, and agencies.

Therefore, an effective emergency prevention and response system has been in operation in the city since 1996. Its operations are led by the mayor of Moscow through the City Government Commission on Emergency Situations and Fire Safety, which coordinates the activities of all services. The Main Administration for Civil Defense and Emergency Situations is the operating arm of the commission.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Since the system was created we have done a certain amount of work aimed at ensuring the security of the capital's residents and territory. This work includes the creation of a regulatory and legal base that relies on international and federal experience. The Law on Protecting the Population and Territory of the City of Moscow from Natural and Non-Natural Emergency Situations and the Concept for the Security of Moscow have both been ratified. These documents defined the system of views of the city's leadership for ensuring the security of its residents. In the process of developing them, several programs were worked out, including Moscow's Radiation Security, Moscow's Chemical Security, Moscow's Fire Security, the Program for the Development of the Moscow City System for Emergency Prevention and Response, and the Program for the Construction of Rescue and Treatment Complexes on the Water. At present, more than 100 regulations and legal acts govern the activities of executive branch agencies, local government entities, and the city's organizations and institutions with regard to protecting the population against emergency situations. These documents have laid the foundation for resolving problems associated with reducing the risk of various types of emergency situations.

Regarding the construction and renovation of structures, primary attention is focused on the implementation of modern technical means of ensuring safety. Work is being done at facilities that use dangerous chemical substances to equip them with automated emergency emissions control systems capable of detecting the onset of an emergency at its early stages and providing a solution to deal with the situation without any human involvement.

At the city level, a light detection and ranging-based automated system for remote monitoring of the condition of the city's air basin has been created and is currently functioning and being further developed. This system makes it possible to automatically detect the initiation of a crisis situation (fire, explosion with release of poisonous substances, contamination of the atmosphere by vehicles and industrial enterprises, and so forth), monitor its development in real time, and predict its effect on neighboring areas.

City government agencies are devoting special attention to ensuring the security of residents in areas where large numbers of people gather and in the city's underground spaces, especially on the metro and in tunnels.

Given that a large quantity of special cargo (gasoline, reagents for refrigeration units, and so forth) is transported through Moscow, as in other cities throughout the world, we have instituted stricter controls over their shipment via truck and rail within the city limits. Furthermore, we have begun creating comprehensive vehicle inspection stations at entry points to the city, with their tasks being as follows:

- checking vehicles for contamination with hazardous substances
- decontaminating vehicles contaminated with hazardous substances
- monitoring the environment

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

However, practice shows that even with the most perfect monitoring systems, it is impossible to fully rule out the possibility of accidents and guarantee the safe operation of a particular facility. Therefore, in order to reduce the degree of risk, in addition to measures aimed at preventing accidents, we must consider a range of measures to reduce the risk that they will occur. Technical and organizational measures should be taken into account.

For example, after the tragic bombing in the underground walkway at the Pushkinskaya Metro Station, we discovered that 80 percent of the victims were injured by flying building fragments or pieces of glass. With this in mind, as part of international cooperation efforts, the Moscow city government is purchasing a unique protective coating for glass that prevents it from breaking. This coating is being installed in areas where large numbers of people gather. The creation, training, and development of emergency personnel hold an important place in the operation of the system. With the support of the Russian Ministry of Emergency Situations, the city has created a modern rescue service, which it maintains at its own expense. About 14,000 firefighters, rescue personnel, and other specialists of the Main Administration for Civil Defense and Emergency Situations are working to ensure the security of Muscovites as they go about their daily affairs. Each day, about 1,700 people report for 24-hour duty shifts, of whom more than 1,500 are firefighters, rescue workers, and support specialists.

Current world experience in resolving the problem of preventing and responding to emergency situations in large cities indicates that achieving an optimal result is impossible without the use of aviation technologies. Therefore, the city has created its own aviation structure, which in times of heavy traffic congestion on the main roads will make it possible to deliver rescuers to the emergency zone in a timely fashion and evacuate the injured to the city's health care facilities.

In conclusion, I would like to say that in eliminating the consequences of emergency situations we have gained bitter but nevertheless practical experience in working under extreme conditions. The Moscow city government is devoting a great deal of attention to issues regarding the prevention of emergency situations and the creation of a security system. We are prepared to share this experience and render the necessary assistance in this regard.

Copyright National Academy of Sciences. All rights reserved.

Critical Integration and Coordination Issues in Urban Security

George Bugliarello
Polytechnic University
National Academy of Engineering

The effectiveness of an urban security system depends ultimately on the coordination and integration of all of its components—from sensors to intelligence, from first responders to hardening of potential targets—as well as on its coordination and integration with regional and national security systems.

Integration and coordination are complementary approaches to the goal of creating an organic system for counterterrorism. In integration, components of the system are fused into a single organization under a single command. In coordination, different independent components, such as entities in the public and private sectors, are connected by compacts and other agreements to operate in unison and share resources to thwart the possibility and consequences of terrorist attacks.

Integration and coordination constitute one of the most difficult challenges in urban security, indeed, in any security system, as they span social and technological aspects and their critical interfaces. Clearly, the concerns and measures involved in urban security are of concern also to government jurisdictions beyond cities, but the purpose of this paper is to focus specifically on some of the major critical issues in achieving such coordination and integration in a city. They include

- unified command and control
- integration of telecommunication systems to provide compatibility, availability, and redundancies
- coordination of the resources of the private sector with those of the public sector (public-private coordination)
- coordination of different administrative jurisdictions

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- local coordination of security approaches in specific areas of a city that encompass significant potential targets of terrorist attacks
- urban security-university interfaces
- public awareness, communication, and education
- identification and protection of critical terrorist supplies
- dual-purpose integration

UNIFIED COMMAND AND CONTROL

Organization of the systems involved in the array of urban security tasks, from prevention to emergency response to recovery, may vary from city to city and from country to country, but the imperative in every case is that in an emergency the command and control of those systems be coordinated and unified. A key question is where the decision making resides and how the staff of the top decision makers is organized to coordinate the responses (Figure 1). This has to do specifically with the architecture of the relation between the city's top decision makers—typically the mayor—and the first responders and emergency managers. Figure 1 shows three examples of architecture from among the many possible. They are characterized by different schemes for relating the first responders

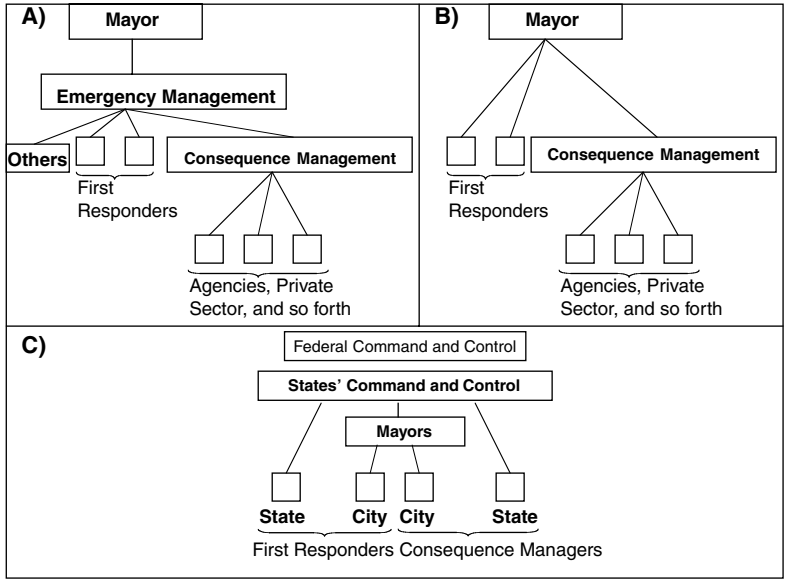


FIGURE 1 Three command and control architectures.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

and the consequence managers (such as offices of emergency management [OEMs]) to the mayor and, in Architecture C, to higher levels of command and control authority. In Architecture A, the mayor is the ultimate authority, as is usually the case, but an emergency management control center relieves the mayor and his or her immediate staff of more detailed involvement in coordinating the inputs of the first responders and the consequence management activities. Architecture B characterizes the situation in New York City, where the first responders (police, fire departments, and emergency medical services) operate in parallel to the OEM, which is responsible for consequence management and coordinates a large number of agencies and private sector organizations. The first responders respond directly and report to the mayor in parallel with the OEM. This arrangement presents more operational complications than one where there is an overall coordinator of emergencies reporting directly to the mayor—a unified command center supporting the mayor's decision making. However, in New York City, the connection between the mayor and the OEM is strengthened by a deputy mayor, and, if necessary, the mayor, being located in an emergency in the OEM. In Architecture C, which can complement other architectures such as those shown in A and B, higher jurisdictional levels (state, federal) can be involved in the command and control and coordination of lower levels—cities and even directly first responders and agencies within them.

An effective command and control system requires integration and coordination along time sequences—from the intervention of the first responders after an incident, to the emergency management of immediate short-range consequences of the incident, to the management of long-term consequences. The integration also needs to encompass the planning and prevention activities that produce scenarios and related probabilities (Figure 2).

The importance of coordination in postincident activities was painfully evident during the blackout of August 14, 2003, which affected some 50 million people in the northeastern United States. All traffic light systems in New York City were incapacitated, and the policing of traffic at many intersections was left to individual citizens, who on their own attempted to untangle and regulate traffic.

One of the most difficult tasks in a large urban setting is evacuation. Large numbers of evacuees can overwhelm the logistics and health care resources of a city and require coordination with agencies in other areas. The situation after the recent earthquake and tsunami disaster in the Indian Ocean region has shown how enormous the task can be in a major incident. Multiple incidents, at brief temporal and spatial distance from each other, can further complicate evacuation, and so can the necessary counterflow of incident responders toward the incident site.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

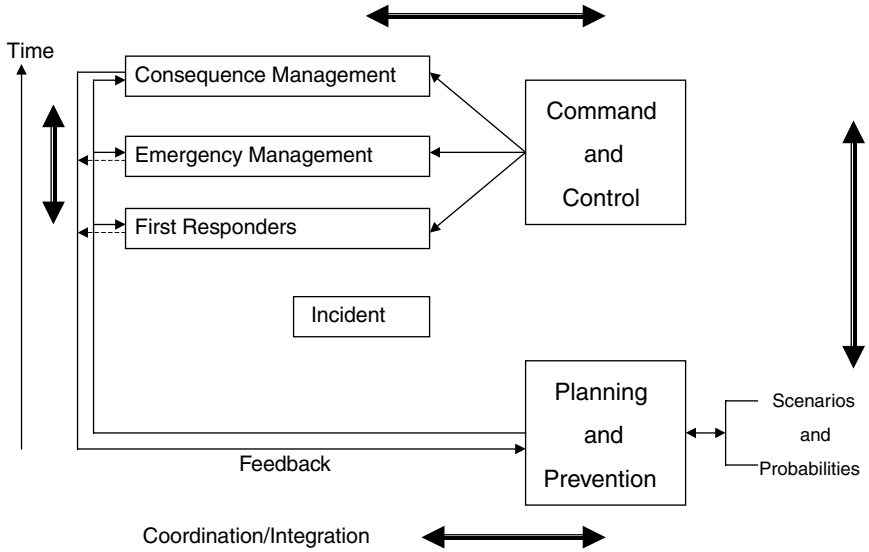


FIGURE 2 An incident's coordination/integration.

TELECOMMUNICATIONS— COMPATIBILITY AND REDUNDANCIES

Telecommunications can be the most vulnerable aspect of urban security. They are essential to making integration and coordination possible. An example on September 11, 2001, in New York City was the inability to reach firefighters in the twin towers and the incompatible frequencies of the fire department and the police department.

Extraordinary volumes of cellular phone calls, which are typical of incidents, can lead to gridlock; hence the need, through coordination, to utilize a multiplicity of networks, including private business networks. Preferential access for priority communications and alternative channels of communication need to be provided, and critical components of the multiple communications system should not be placed in the same location, as they were on September 11, 2001. In the August 2003 electric power blackouts, agencies in New York City that relied on cellular phones could not reach members of their own staffs. The situation is now being addressed by the creation of a dedicated network for city agencies and other critical entities. Communications security also involves cybersecurity, the physical integrity of the network, and the ability to minimize terrorist denial of service actions, whether they are the ultimate goal of an attack or serve as a preliminary to other terrorist acts.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

PUBLIC-PRIVATE COORDINATION

When a large part of the infrastructure is in private hands, as in the United States (for example, about 80 percent is private in New York City) there is a need to coordinate it with the public agencies involved in incidence response. Insurance companies are largely private and can have a significant role in the security of a city. For instance, they can provide incentives to encourage the private sector to strengthen the security of its buildings through the use of guards, cameras, and sensors as well as other measures, such as barriers and reinforced structures. Coordination with nongovernmental organizations (NGOs) in planning and consequence management is another important facet.

Public-private coordination is also important for incident management inside private organizations and for recovery operations. For instance, the clearing of debris from a major incident is often beyond the capacity of municipal services and requires utilization of private sector enterprises. After the World Trade Center attack, private engineering firms assisted the city in assessing damage and planning recovery, and private construction and earthmoving and carting companies were engaged to secure damaged sites and remove the large amount of debris created by the collapse of the World Trade Center buildings.

Insurance companies could be significant in recovery operations, too, as with fallout of radioactive material on the roofs of buildings and other surfaces. Depending on the nature of the materials that constitute these surfaces, the radioactive fallout might react with those materials, making it imperative to remove it as rapidly as possible before reactions take place that incorporate radioactivity in the surface material. Insurance companies could influence the safety and security of buildings by offering incentives in the selection of the material used in the roofs and in encouraging speedy removal.

COORDINATION OF DIFFERENT ADMINISTRATIVE JURISDICTIONS

In many larger cities, the city center and the outlying areas—still part of the metropolitan complex—are under different jurisdictions, making coordination of their preparation and their responses quite complex (Figure 3). In the case of New York City, for example, Greater New York extends to New York State counties in Long Island and to the north of the city, each with its own incident prevention and response organization, as well as to counties in two other states, Connecticut and New Jersey. All these areas are bound to be profoundly affected by an attack on the city center, for example, in a potential evacuation. Similarly, in Washington, D.C., the District of Columbia borders on the states of Maryland and Virginia. In New York, New Jersey, and Connecticut, the coordination of emergency responses is facilitated by a Federal Emergency Assistance Compact. In New York and New Jersey, the Port Authority of New York and New Jersey

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

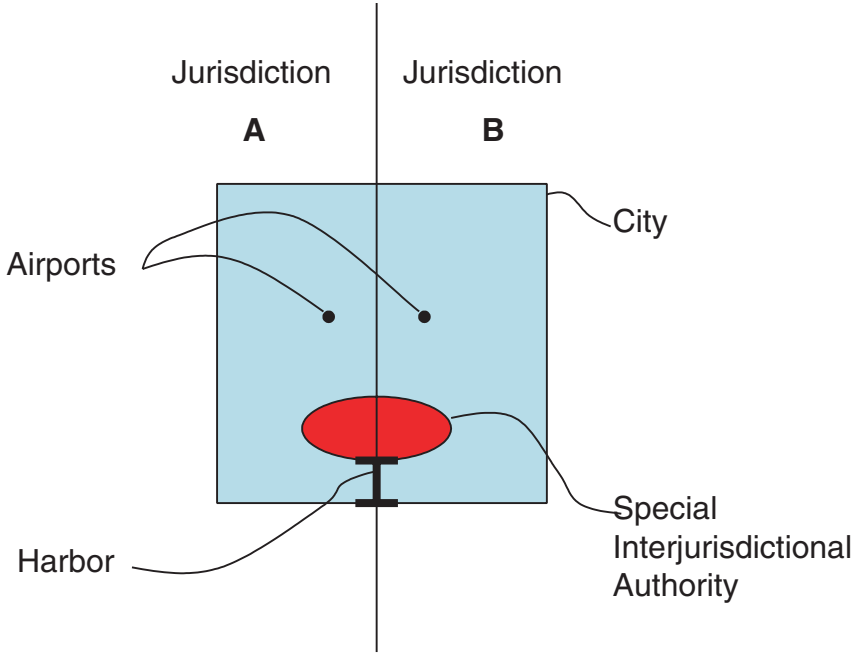


FIGURE 3 Multiple jurisdictions, requiring multiple levels of coordination.

has jurisdiction over the harbors and airports of the metropolitan area, and responsibility for their security. (The waterways of the metropolitan area are patrolled also by the U.S. Coast Guard.) Thus special authorities like the Port Authority are an important coordination and integration mechanism. They might have their own security forces, their own land, their own buildings, and their own architectural and operational standards. This, however, can also have negative consequences, if some of their standards are different from those of the city, as with the stairways in the World Trade Center twin towers. Coordination of the complex of transportation, pedestrian movements, emergency responders, shelters, and logistic support becomes even more challenging in the evacuation of several areas, whether contiguous or in other portions of the city, and whether these events are simultaneous or sequential.

Apparently, thus far, no major city worldwide has an effective evacuation plan for the entire city, but at best has only plans for partial evacuation. Evacuation, among its many aspects, requires providing simultaneous access to first responders and coordination of traffic lights through the areas of concern and often through much of the city. In the United States a complex issue with a still not fully fathomed impact is the interaction and coordination of urban security

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

systems with the complex organization of the recently established U.S. Department of Homeland Security.

Coordination and integration of different jurisdictions are necessary to protect the extended footprint of concern for a city's protection. On September 11, 2001, that concern clearly would have extended beyond New York City and Washington, D.C., to airports, such as the airport in Boston, conveying passengers to these cities. In terms of ports, the footprint encompasses not only the ships entering harbors but also the inspection and certification at ports of origin, as well as the protection from blockages of waterways logistically critical to the city. Transshipment points, where goods are transferred from conveyance to conveyance, whether at sea or land, or in the transport of baggage from airline to airline, are other potential terrorist penetration points of concern to the security of cities. On trains, as in the Madrid attack, the footprint encompasses places outside the city itself, where terrorists might board or implant devices. Electrical and telecommunications networks, with their long geographic span, are also part of the footprint of concern.

LOCAL COORDINATION

In every city there are special areas encompassing a multitude of uses and diverse institutions that are critical to security or are potentially rich targets. An example is Metrotech in New York City (Brooklyn; see Figure 4), with different

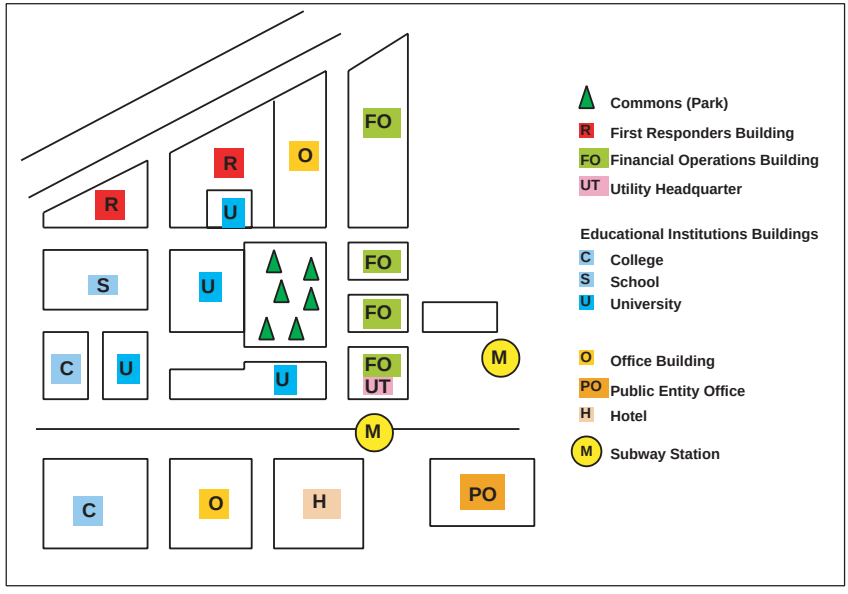


FIGURE 4 A site requiring local integration (Metrotech).

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Box 1
Local Integration Components

Preventive Measures
- Barriers architecture
- Sensor networks
- Telecom security
- Surveillance

Incident Management
- Command and control systems
- Evacuation procedures
- Emergency medical resources
- Emergency shelters
- Rescue operations
- Emergency communication networks and ad hoc networks
- Debris removal services
- Utilities and other infrastructure emergency repair capabilities

entities of different characteristics, both public and private, that need to be coordinated in the prevention of and response to a terrorist act. In a small area of fewer than 20 acres, Metrotech encompasses critical police and fire department facilities (the 911 emergency telephone hot line, and the headquarters of the city's fire department and Department of Information Technology); business offices; institutes of higher education; a school; highly technological financial services facilities; a hotel; commercial establishments, such as restaurants and other shops; multiple subway lines and stations; and crowded road and pedestrian traffic. A major incident in such a dense and diverse area could force evacuation to street level of up to 30 thousand people. Each component of Metrotech has its own emergency plan, but for an incident affecting the entire area, such plans need to be coordinated with those of the other entities in the area, for example, to identify other security risks common to the area and to reduce the possibility that the large potential population brought out of the buildings and subways in the emergency might itself become the target of an attack. It is important to identify throughout a city similar local areas or districts that might require a coordinated plan and to determine the components of such a plan (see Box 1). Entertainment centers, utilities installations (for example, Figure 5) and transportation hubs (major stations and airports), with all the other activities they attract around them, are other examples of environments where local integration is critical for a more effective response. A focus on local coordination also facilitates surveillance, dual-purpose integration, and the identification of potential terrorist supplies.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

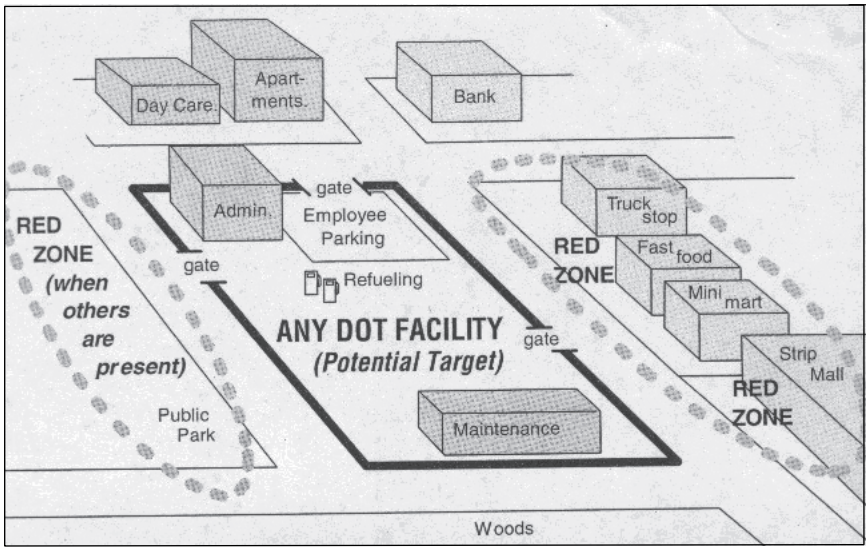


FIGURE 5 Local integration: example red zones around a transit facility (Department of Transportation). Source: Transportation Research Board. 2004. P. 6 in NCHRP Report 525, Surface Transportation Security Volume 1—Responding to Threats: A Field Personnel Manual. Washington, D.C.: Transportation Research Board.

URBAN SECURITY-UNIVERSITY INTERFACES AND COORDINATION

Universities can be a very useful component of the security defenses of a city and should be included in a coordinated approach to security. The university's multiple functions and capabilities and their relation to urban security needs and tasks are shown in Box 2. Other educational and research entities, such as colleges, scientific institutes, and even specialized secondary schools, can also carry out a number of these functions, even if not to the same extent as a university. In various measures, all these institutions can—and many do—research issues pertinent to urban security and train and prepare personnel at all levels, from security staff to fire protection engineers, from structural engineers to decision makers (Hall, 2004). They can enhance public awareness of urban security and engender public trust, since they are generally perceived as neutral ground that can serve as a convener of discussions and examinations of urban security policies. A problem, however, for which for now appears to have no clear solution, is how to deal with access to sensitive, even if unclassified, information by faculty and students working on security projects.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Box 2
Capabilities and Potential Role of a University in Urban Security

University Capabilities
- Education
- Training
- Research
- Consulting
- Public outreach
- Convening capability
- Databanks
- Facilities (special classrooms, laboratories)
- Policy studies

University Responses to Urban Security Needs
- Preparation of leadership
- Specific training and perhaps also an ROTC for urban security (decision making, fire protection, infrastructure managers and engineers, distance learning)
- Research
- Information services
- Response to specific security demands

PUBLIC AWARENESS, COMMUNICATION, AND EDUCATION

Beyond injuries, death, and physical damage, the greatest impact of terrorism is the psychological effect, as it amplifies manyfold the material effect of an attack and is difficult to counteract. The media have a major role in informing and educating the public and reducing the likelihood of panic. For instance, group psychology during an incident may lead to patterns of behavior that impede the response and strain logistic systems. Many media outlets are respected for their accuracy, even though some contribute to panic with sensationalism.

Even first responders and emergency management organizations might not communicate as effectively as the media, business, and NGOs, and might, at times, be mistrusted. Usually more trusted are institutions that naturally have an educational and instructional function, such as schools, colleges, universities, and professional societies. These institutions can reach into the general public at many levels, but thus far have been involved only to a limited extent in conveying to the public a realistic understanding of terrorist actions and their real impact. Thus, fostering their interaction with terrorism experts, researchers, first responders, and emergency managers is a critical component of a coordinated response to urban terrorism that needs to be addressed systematically and on a broad front (Figure 6).

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

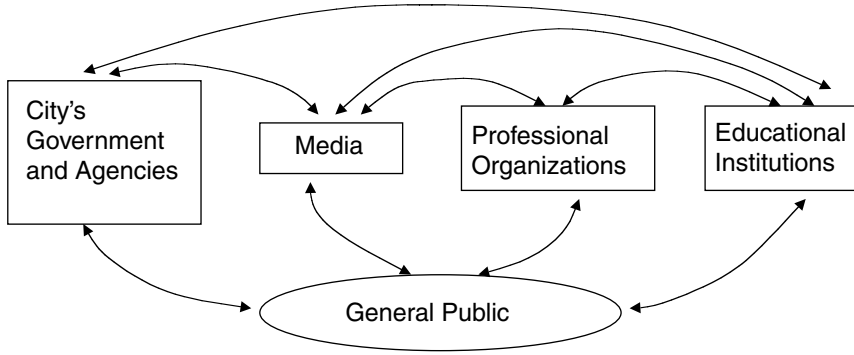


FIGURE 6 Public communication system synergies.

Employers, too, can contribute to the timely diffusion of important information to their dependents, and beyond them, as in a program encouraged by the OEM in New York City. The importance of such connections is evident, for instance, if one considers the lack of a realistic understanding by the general public about dirty bombs or of how to protect oneself from a biochemical attack that could lead to panic and other psychological impacts.

In this context, in the United States, the Office of Public Information of the National Academy of Engineering has conducted in several cities a series of well-reported awareness exercises, through simulated incidents, to prepare the media to report on an attack in a realistic and balanced way (see "News and Terrorism: Communicating in a Crisis" by Randy Atkins, in these proceedings).

IDENTIFICATION AND PROTECTION OF POTENTIAL TERRORIST SUPPLIES

A city possesses a broad array of resources—explosive material, biological agents, chemical factories and stores, radioactive sources, electronic devices, vehicles, fire weapons, and so forth—that can be misused by terrorists to attack objectives within the city (Box 3). In the United States, most of these supplies are in private hands. The responsibility for their protection—often not carried out very effectively—needs to be integrated with responsibilities of the public sector. Many potential supplies can be easily identified, but their protection is generally spotty and represents a critical dimension of an integrated approach to urban security. Also, coordination of the surveillance activities carried out at the neighborhood level by stores, individuals, and local organizations (such as in New York City the Business Improvement Districts [BIDs]) can be very helpful in complementing larger scale citywide endeavors carried out by police forces, industry, large business organizations, and specialized agencies.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Box 3
Potential Terrorist Resources in a City

University, College, and Other Educational Institutions
- Electronic devices
- Chemical supplies
- Biological organisms
- Computers and access to networks
- Sensitive information

Hospitals
- Chemicals
- Biological organisms
- Radioactive sources

Transportation Infrastructure
- Cars
- Trucks
- Gasoline tanks

Chemical Industry and Chemical Stores
- Toxic material
- Chemicals
- Explosives
- Poisons

Energy Utilities
- Liquefied natural gas
- Gas pipelines
- Nuclear materials

Financial Institutions
- Money

Electronic Stores
- Devices (sensors, batteries, microwave generators)

Ports
- Boats and ships
- Storage facilities

Airports
- General aviation

Libraries and Databanks
- Sensitive information
- Data tampering possibilities

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

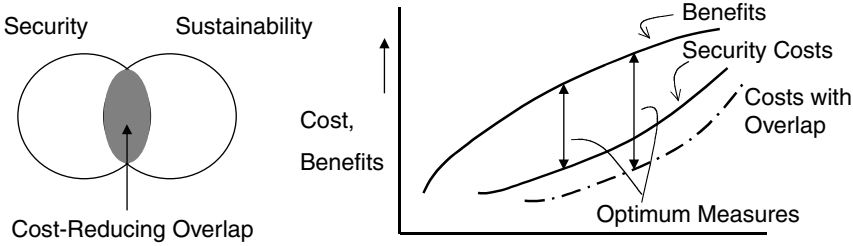


FIGURE 7 Security-sustainability integration.

DUAL-PURPOSE INTEGRATION

In the long term, the costs of urban security measures can become very large. To reduce the burden, it is increasingly important to find ways to integrate security measures with measures to satisfy other urban needs (NRC Committee on Science and Technology for Countering Terrorism, 2002). For instance, a long-term need of increasing concern to every city is to sustain its achievements in the future. The intersection of security and urban sustainability concerns identifies a common ground (Figure 7) that can reduce the combined cost of both. Thus a possible goal in developing an urban security system could be to integrate it as much as possible with sustainability measures. Figure 7 shows how, hypothetically, an overlap of the two can increase the benefit-cost difference of a security system. Examples of measures that can reduce urban security costs through integration with other needs include building designs; more effective maintenance; multipurpose guards and surveillance personnel; and multi- or dual-purpose sensors for security, traffic monitoring, air pollution, fire detection, and store surveillance.

TWO META-ISSUES: HUMAN-MACHINE AND SECURITY-CIVIL LIBERTIES INTERFACES

Human-machine integration and the interface of protection, laws, and civil liberties are two meta-issues critical to effective integration of urban security systems, but can only be briefly mentioned here. In terms of human-machine integration, the complexity of a city and the multiplicity of agencies and organizations involved in its security makes it imperative to utilize machines—software and hardware—as much as possible, to help decision makers, first responders, and others. The difficult question is how to create the most effective interfaces.

The interface between security and civil liberties is one of the most sensitive areas in urban security, as it ultimately determines the level of security and of

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

command and control a community is willing to accept in the creation of an effective response to terrorist threats. This requires a close dialogue between the exponents of the city's civil values and the entities entrusted with the security of the city, to reach a modus operandi acceptable to both.

CONCLUSION

In brief, the extent to which different aspects of coordination and integration, such as those set forth in this paper, are carried out is a measure of the effectiveness of an urban security system. Coordination and integration are essential for reducing the probability and impact of terrorist attacks, but they are also essential for lessening the impact of natural disasters and for enhancing the long-term sustainability of a city.

REFERENCES

Bugliarello, G. 2003. Urban Security in Perspective. Technology in Society, November, 25(4): 499–507.

Hall, R. 2004. Protecting the Home Front. University Research Helps Keep Us Safe from Threats from Abroad. Prism, October 2004:44.

NRC Committee on Science and Technology for Countering Terrorism. 2002. Making the National Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Special Characteristics of Firefighting in Urban Areas

Nikolay P. Kopylov
Scientific Research Institute for Fire Prevention Defense of the
Russian Ministry of Emergency Situations

In urban areas, terrorist attacks are aimed at civilian targets with many people, such as residential structures (apartment building bombings in Moscow, Volgodonsk, and Buinaksk), theatres (the *Nord-Ost* theater), schools (the Beslan elementary school), business centers (the World Trade Center buildings), and rail and subway trains (Spain, Moscow, South Korea, and Tokyo). The main purpose of terrorist attacks is to kill and harm as many people as possible.

In most cases, attacks on such objects cause fires. The situation can develop according to several possible scenarios:

- impact—explosion—fire (World Trade Center)
- explosion—fire (apartment building on Guryanov Street in Moscow; Beslan elementary school)
- arson—fire (South Korean subway)

Firefighting and rescue activity during a terrorist attack are affected by special factors not common in usual firefighting and rescue practice. Explosions partially or completely destroy buildings, which changes the fire development scenario, decreases the fire resistance of structures, and causes hazards for firefighters, rescue workers, and civilians. In a terrorist attack, there is a strong need for the immediate evacuation of large numbers of people from the area, which becomes a difficult task in situations of panic, inappropriate mob behavior, and lack of rescue equipment. Sometimes firefighting and rescue operations must even be performed under crossfire (Beslan school). All these factors require special consideration.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

FIRES CAUSED BY EXPLOSIONS

The impacts of the planes striking the World Trade Center buildings caused fuel vapor explosions and fires. Because of the high combustible load value in the area of the fires, high temperatures developed. The fires spread through the damaged and destroyed building structures. The fire-resistant coatings of load-bearing structural elements were damaged, which seriously decreased the fire resistance of the buildings. The summary effect of the impact, explosion, and fire caused the buildings to collapse.

The World Trade Center buildings had a high fire resistance rating of R240 (4 hours) for the external bearing walls and R180 (3 hours) for all other load-bearing elements. Such times (3 hours and more) guarantee the fire resistance of the building, because firefighting systems should extinguish the fire in that time. The impact and explosion decreased the fire resistance of the damaged elements. The major process responsible for the structural collapse was creep flow of the steel elements. Undamaged load-bearing elements took the strain from the destroyed elements, so the creep flow became more intense and the critical point was achieved in less time than under standard fire resistance test conditions. If certain elements are withstanding an additional load, bearing failure can occur when the temperature of the bearing element reaches 400–420 °C. Because the fire-resistant coating of many structural elements in the impact zone was damaged, the rise of structural temperatures to the above-mentioned values led to the collapse of the buildings.

The Russian Scientific Research Institute for Fire Protection has conducted studies involving the modeling of fire development in the damage zone in buildings after airplane impacts. The main purpose of the research was to obtain information necessary for estimating the necessary fire resistance rating for building structures.

The impact of a Boeing-767 into the World Trade Center was considered as a model situation. It was assumed that the crash would result in a 50 × 10 m opening in the external wall and would create an internal hollow measuring 50 × 50 × 10 m. Assuming that kerosene is spilled on the entire floor area of the damaged zone and flashover occurs quickly, an integral fire development model[1] was used for estimating fire endurance time.

The main system of equations consisted of

- mass conservation equation
- energy conservation equation

[1]Koshmarov, J. A., and J. S. Zotov. 1996. Guide for Laboratory Work on the Theme "Fire Hazard Factor Modeling," Part 1. Moscow: School for Military Firefighting Technology of the Russian Ministry of Internal Affairs.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- oxygen balance equation
- fuel component balance equations

The influence of the combustible load on thermal- and gas-dynamic parameters of the fire's development was considered. Three scenarios for fire development were modeled: kerosene fire, furniture fire, and combined furniture-kerosene fire. The dimensions of the enclosure (damage zone) in all three scenarios were 50 × 50 × 10 m. The opening dimensions in the basic scenario are 50 × 10 m.

Kerosene Fire

The fuel tanks of a Boeing-767 are capable of carrying 90 tons of kerosene when fully loaded. That quantity was considered as the maximum quantity of fuel spilled in the enclosure. The temperature dynamic in the enclosure relative to the spilled fuel mass is shown in Figure 1. It indicates that if the mass of spilled fuel is more than 30 metric tons, the combustion process soon stabilizes and is characterized by a certain average ambient temperature in the enclosure. The duration of the stable period depends on the quantity of fuel. Figure 1 also shows the temperature curves for the standard fire endurance test. The modeled fire curve is close to the hydrocarbon (HC) curve, which describes liquid fuel

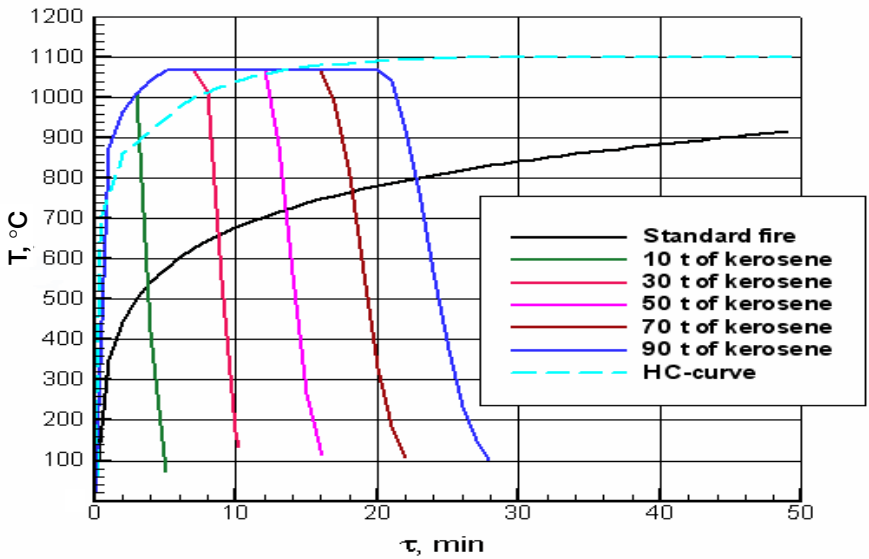


FIGURE 1 Dynamics of average temperature in the enclosure with various quantities of combustible in the form of spilled kerosene.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

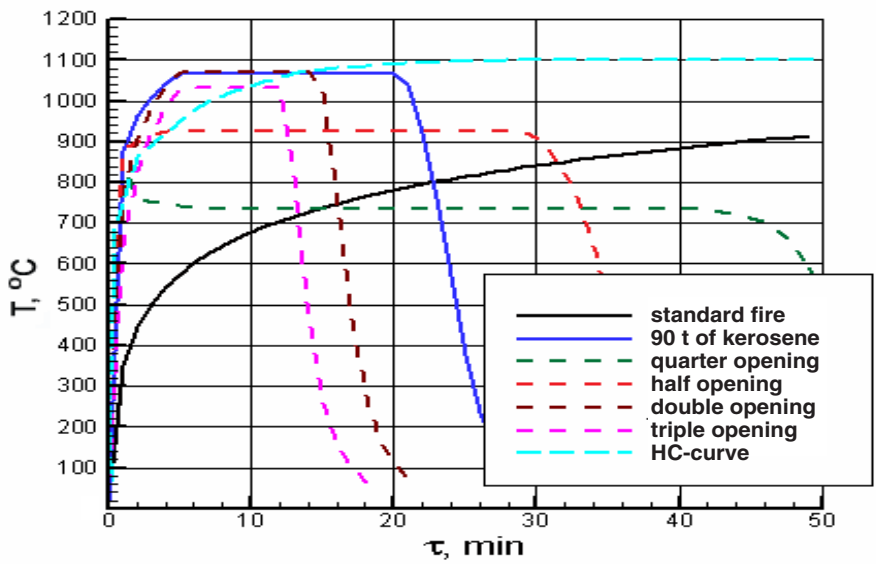


FIGURE 2 Dynamics of average temperature in the enclosure during combustion of 90 metric tons of kerosene with different sizes of opening areas.

fires. If the mass of spilled fuel is less than 10 tons, a stable combustion regime is not achieved because of the lack of fuel.

Figure 2 depicts temperature curves describing the combustion of 90 tons of kerosene in an enclosure with opening areas of various sizes. In the basic scenario, the dimensions of the opening were 50 × 10 m. Other scenarios have different opening dimensions: 12.5 × 10 m (quarter opening), 25 × 10 m (half opening), two openings of 50 × 10 m (double opening), and three openings of 50 × 10 m (triple opening). The last scenario assumes the destruction of three walls in the enclosure and is of no practical importance, but may be useful from a theoretical standpoint.

Figure 2 shows that combustion became stable in all scenarios, but the average temperatures throughout the enclosure are different. The lowest average temperature is achieved when the opening area is minimal, because in such conditions the combustion process is limited by the oxygen supply (so-called ventilation-controlled fire). The temperature rises as the opening area increases, achieving a stable regime (half-opening scenario and basic scenario) as a result of combustion rate growth (Figure 3). Fuel is consumed faster in that case, so the stable regime is shorter. Despite this factor, there is an opposite factor decreasing the average ambient temperature. An increase in the size of the opening area causes an increase in the air supply and dispersion of smoke. The quantity of gaseous nitrogen flowing through the enclosure is also increased, as is the quan-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

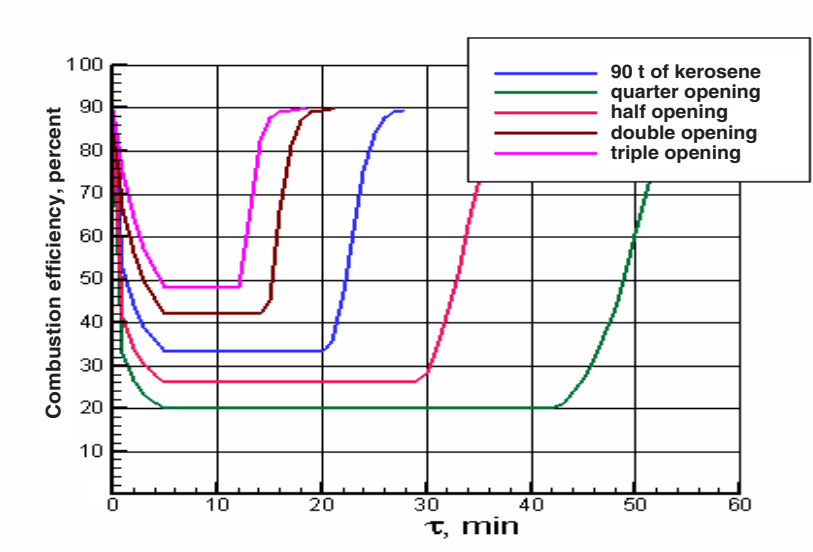


FIGURE 3 Variation of combustion efficiency during combustion of 90 metric tons of kerosene with different sizes of opening areas.

tity of heat accumulated by it. Ultimately, as shown in Figure 4, a point is reached (see curves for basic and double-opening scenarios) when an increase in the size of the opening does not cause a further increase in temperature. In fact, a further increase in the size of the opening decreases average temperature somewhat (the triple-opening scenario).

Dependences of structural temperature on fuel mass and opening area are shown in Figures 5 and 6. They are correlated with ambient temperature dependences.

Furniture Fire

Figure 7 shows average ambient temperature dynamics in an enclosure for a case in which the combustible load is common and consists of furniture. The mass of the combustible load was assumed to be in the range of 30 to 375 metric tons.

The largest value of the combustible load was chosen in accordance with the handbook of Construction Norms and Regulations 21-01-97,[2] which establishes the maximum allowable quantity of the combustible load as 50 kilograms/m^2 (in

[2]Central Scientific Research Institute of Industrial Publications. 1998. Limitation of Fire Development, Construction Norms and Regulations 21-01-97; Fire Safety of Buildings and Structures, MDS-21-1.98. Moscow: State Unitary Enterprise ZPP.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

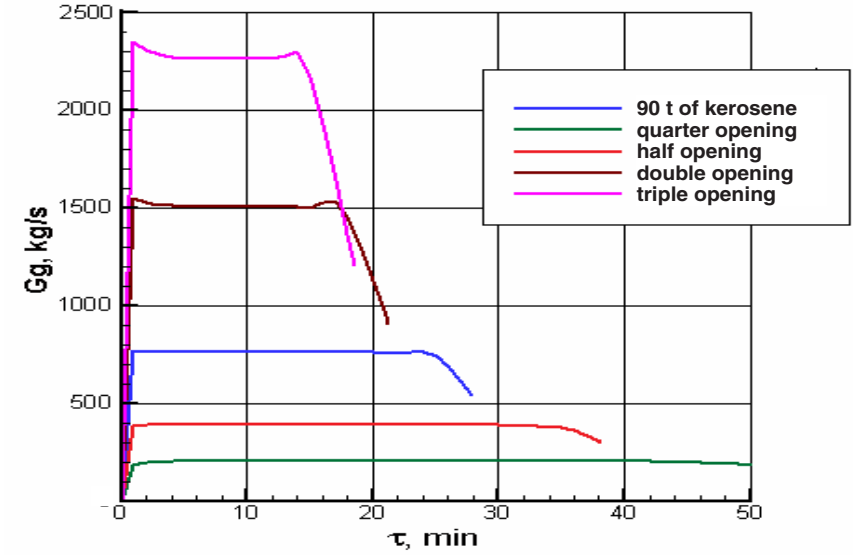


FIGURE 4 Dynamics of mass flow of gas emissions (Gg) during combustion of 90 metric tons of kerosene with different sizes of opening areas.

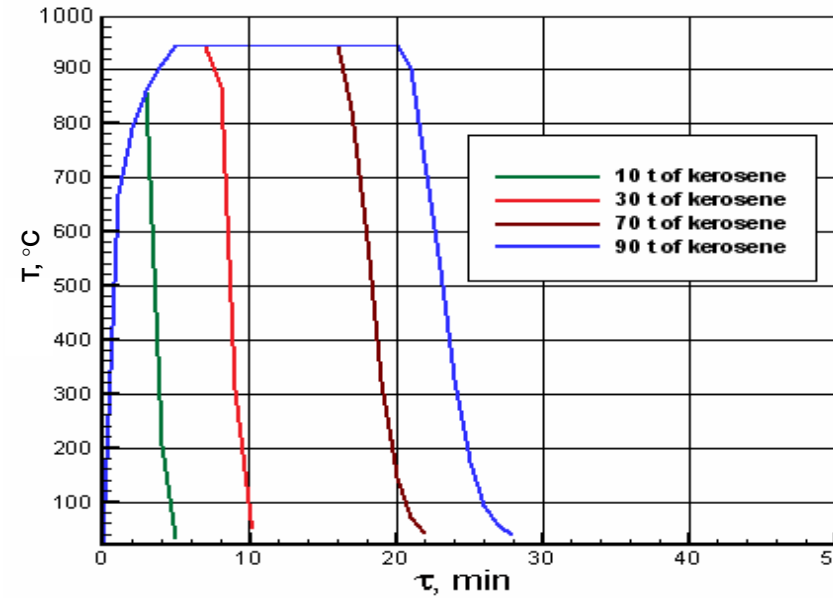


FIGURE 5 Dynamics of the temperature of the enclosure walls with different quantities of combustible spilled kerosene.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

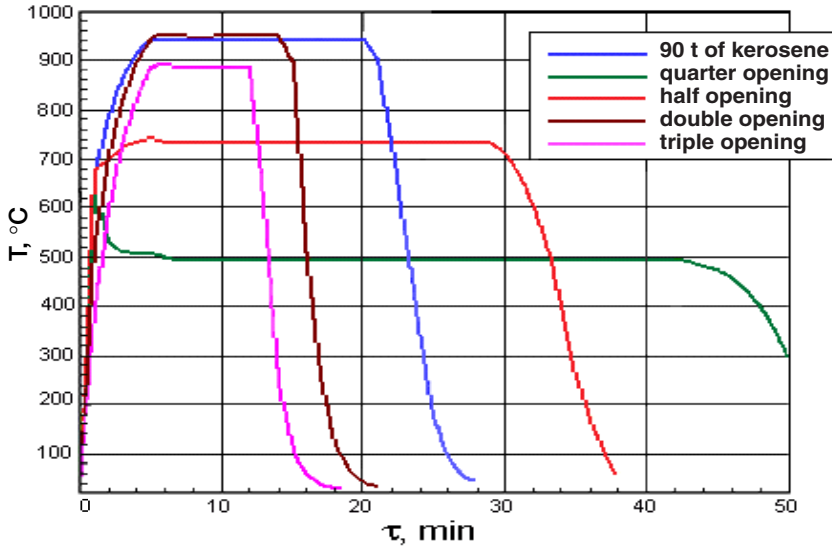


FIGURE 6 Dynamics of the temperature of the enclosure walls during combustion of 90 metric tons of kerosene with different sizes of opening areas.

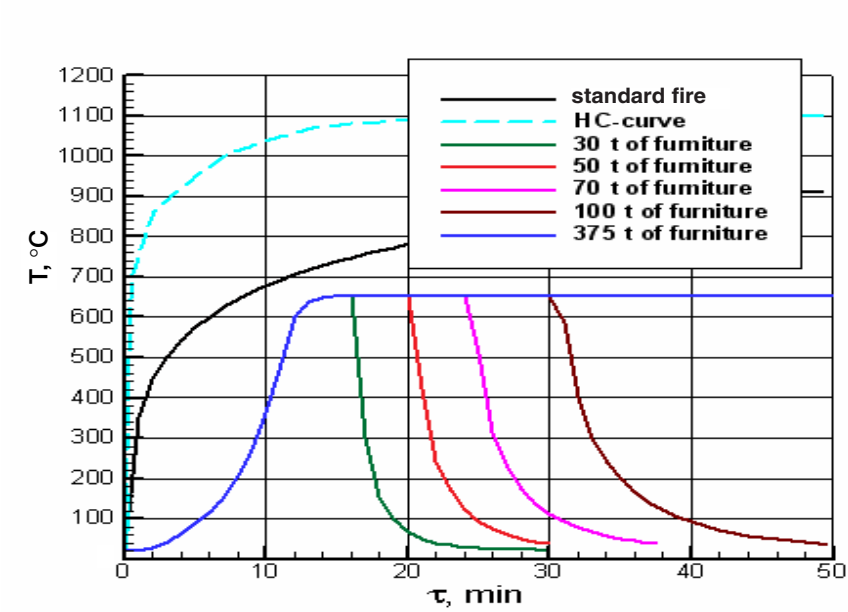


FIGURE 7 Dynamics of average temperature in the enclosure with various quantities of furniture.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

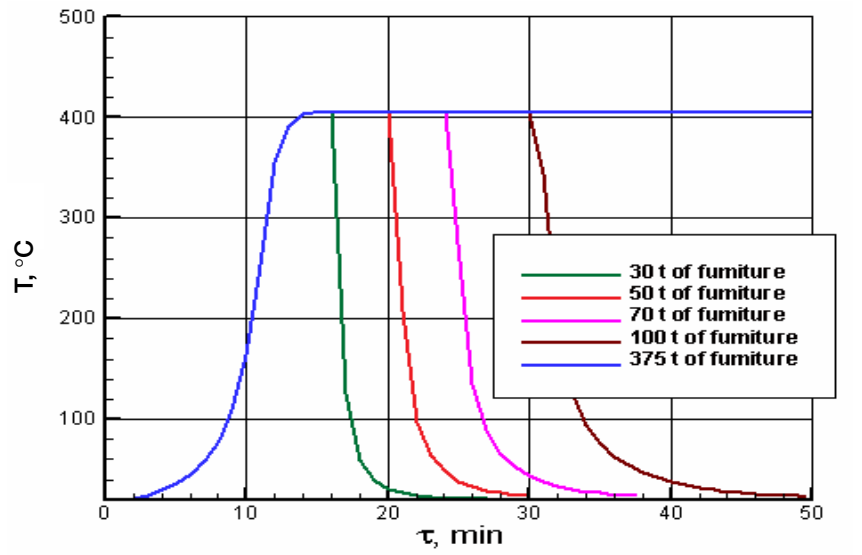


FIGURE 8 Dynamics of average temperature of the enclosure walls with various quantities of furniture.

wood). Thus, given that the floor area of that enclosure (damage zone) equals 2,500 m^2 and after the impact the combustible load in the damage zone is accumulated from three floors of the building, the total mass of the combustible load in the damage zone equals $50 \times 2{,}500 \times 3 = 375{,}000$ kg. Figure 7 shows that the temperature dynamic of the furniture fire has the same pattern as the temperature dynamic of the kerosene fire. A stable regime is achieved later than with the kerosene fire because the furniture fire spreads more slowly. The construction temperature curves for the furniture fire correlate well with the curves for the kerosene fire (Figures 7 and 8).

Combined Kerosene-Furniture Fire

Temperature-time dependences for different kerosene-furniture ratios are shown in Figure 9, which indicates that the maximum temperature is achieved during a pure kerosene fire and the minimum temperature during a furniture fire. When a combined kerosene-furniture load is burning, intermediate temperature values are achieved. It is worth noting that decreasing the kerosene ratio in the combustible load from 1 to 0.25 causes the temperature to fall by only 50 °C.

If the quantity of the furniture load meets standard requirements, the kerosene ratio is less than 25 percent even if the airplane fuel tanks are full. Thus, in most probable fire scenarios, temperature depends to a considerable extent on kerosene mass.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

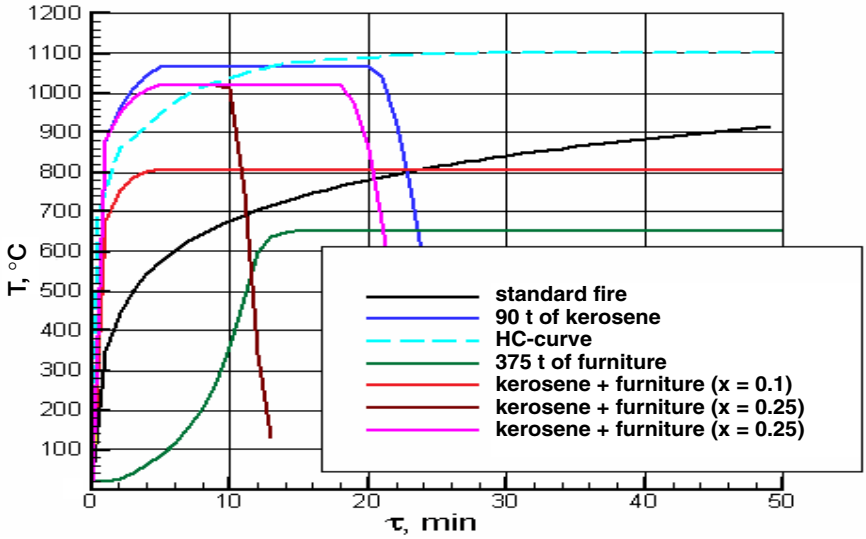


FIGURE 9 Dynamics of average temperature in the enclosure with various quantities of kerosene in the combustible load.

For a combined combustible load, as for a pure combustible load, an increase in the combustible load mass causes an increase in the stable combustion time without affecting the ambient temperature.

Temperatures of the structures are shown in Figure 10. Assuming that steel elements collapse when their temperature rises to 500 °C (± 50 °C; such an assumption is widely used in practice), with a kerosene ratio of more than 10 percent, the collapse should occur in the first minutes after the impact. In reality, the World Trade Center buildings resisted the fire for 56 minutes and 1 hour 43 minutes, respectively, before collapsing. This could occur if the mass of the kerosene burned in the damage zone was no more than 37.5 metric tons. That result correlates with U.S. researchers' estimates that each plane had approximately 30 metric tons of fuel onboard prior to impact.[3]

Estimate of Fire Endurance of the Damaged Construction Elements

Experimental studies were conducted to estimate the effect of mechanical damage on fire resistance time for two types of structural elements: floor panels

[3]Hamburger, R., W. Baker, J. Barnett, J. Milke, and H. B. Nelson. 2002. WTC1 and WTC2. World Trade Center Building Performance Study. Washington, D.C.: Federal Emergency Management Agency.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

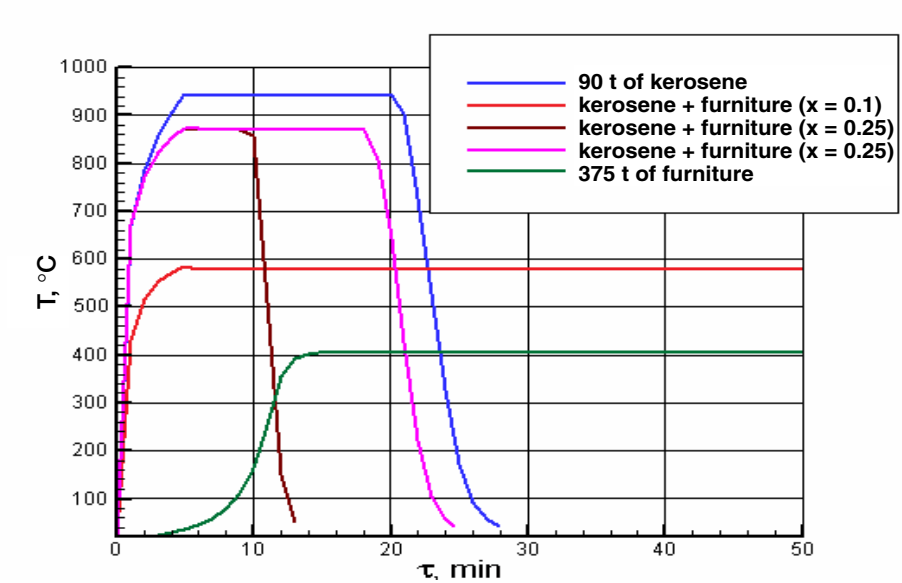


FIGURE 10 Dynamics of the temperature of the enclosure walls with various quantities of kerosene in the combustible load.

and bearing columns. Ten floor panels with dimensions 5.1 × 1.2 × 0.22 m made of M200 heavy concrete and three central compressed columns made of M300 heavy reinforced concrete with granite gravel were tested. Both types of elements were subjected to mechanical damage—cracks and chips exposing reinforcement bars. Tests were conducted according to standard procedure; the floor panel loading was P_{panel} = 1,067 kg/m^2 and the column loading was P_{column} = 120 tons.

The test results are presented in Figure 11 and Table 1.

Mechanical damage to the floor panels greatly decreases their fire resistance time. Hollow-core panels with 2-millimeter reach-through transverse cracks have 21 percent less fire endurance time than undamaged panels. A transverse chip at the middle or on the edge of the panel exposing half the diameter of the reinforcement bar decreases fire endurance time by 23 percent. A 200-millimeter transverse chip at the middle of the panel exposing half the diameter of the reinforcement bars decreases fire endurance time by 50 percent.

The higher the exposure coefficient for the reinforcement bars, the lower the fire endurance time for the damaged column (for α_e = 0.03, fire endurance time falls by 6 percent, and for α_e = 0.14, fire endurance time falls by 21 percent). In addition, armature exposure causes column instability when a load is added. All of this may cause column-bearing failure in a fire.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

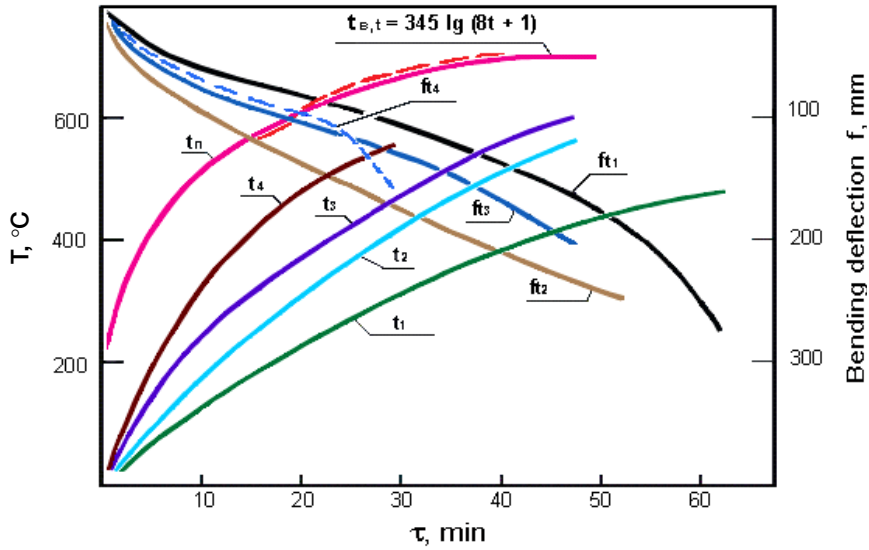


FIGURE 11 Temperature change and maximal bending deflection during fire resistance testing of hollow-core slabs.
Note: $\mathbf{t_{B,t}}$—standard temperature fire regime, °C; $\mathbf{t_n}$—actual temperature of the fire chamber, °C; $\mathbf{t_{1,2,3,4}}$—average values of the reinforcement heating, °C; $\mathbf{ft_{1,2,3,4}}$—bending deflection in the middle part.

TABLE 1 Theoretical and Experimental Results of Column Fire Resistance Estimates

Reinforcement bar exposure coefficient α_e	Fire resistance time τ, min.
0	170*
0.03	160
0	140*
0.03	130
0.14	110

*theoretical value

Fires in Piles of Wreckage

After a building collapse caused by a bomb explosion, fire often occurs in the wreckage. Victims trapped in the rubble may suffer from all of the hazard factors inherent in fire: high temperature, combustion products, and flame. The fire may also cause wreckage shifts as it progresses.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

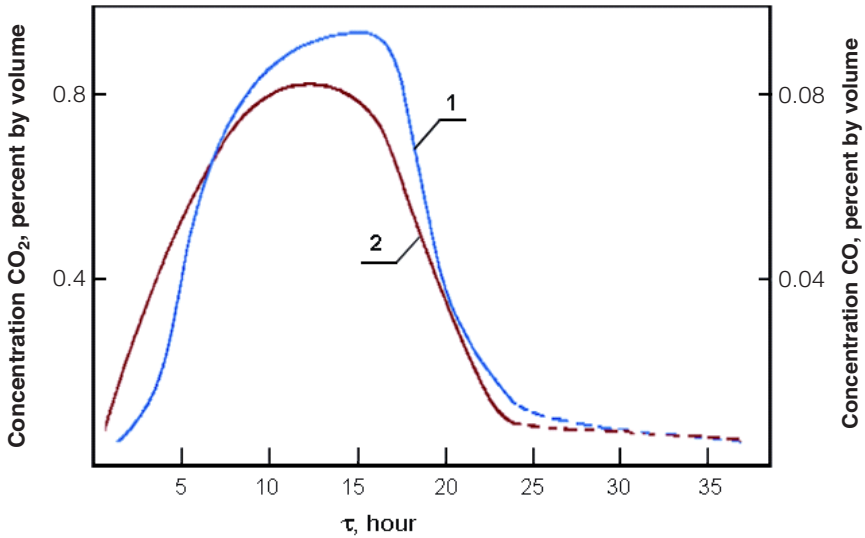


FIGURE 12 Average CO and CO_2 concentrations at fires in the ruins of a one-story brick building of the second fire resistance class.
Note: **1**—CO concentration; **2**—CO_2 concentration.

Figure 12 shows an average of experimental data illustrating the dynamics of fire hazard factors (CO and CO_2 concentrations). Local concentrations at certain points in the piles of rubble may be much higher than the values shown. Therefore, rescue and firefighting operations should be performed quickly in order to save as many trapped victims as possible.

Subway Fires

Crowds of people, a limited number of evacuation exits, long evacuation paths, and fast-changing hazard dynamics during a fire make subway stations and trains especially dangerous places. It is well recognized that the most dangerous fire development scenario in a subway is a fire in a train that causes it to stop in a tunnel. Such fires occurred in 1991 in St. Petersburg and in 1994 in Moscow. It was only because there were no people onboard the trains that the fires did not lead to catastrophes.

Such a catastrophe occurred in a Baku subway tunnel on October 28, 1995. A train with 700 aboard caught fire between Ulduz and Narimanov stations; 300 people died and 270 were injured. This is the most terrible fire of that sort to date.

Until 2003 it was believed that fires in subway stations equipped with fire protection systems and evacuation exits cannot cause mass fatalities. However,

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

the arson fire that occurred on February 18, 2003, at Jungangno station of the Daegu city subway in South Korea caused 196 deaths and dozens of injuries. The fire started on a train at a station during rush hour (a second train was also stopped at the same station). Later investigation revealed that the high number of victims was caused by the inappropriate actions of train and station personnel.

In recent years, subway trains have become more frequent targets of terrorist attacks. The Tokyo subway was attacked by terrorists using poisonous gas (sarin). At approximately 8:00 a.m. on March 20, 1995, containers full of liquid emitting poisonous gas were placed simultaneously on trains on three lines—Hibiya, Marunouchi, and Chiyoda. Symptoms of the poisoning included fainting, vomiting, and eye pain; 12 people died (2 of them subway personnel) and approximately 5,600 were injured. Many rescue teams responded to the accident. The Tokyo fire department directed 340 rescue and chemical control units to 15 subway stations. The total number of people engaged in the operation was 1,364. Rescue and chemical control workers rendered first aid to victims at the scene and carried out tasks related to evacuating people, deactivating the gas-producing liquid, and analyzing the poisonous gas. A total of 131 rescue units saved 692 people, 688 of whom were hospitalized. Because the chemical composition of the poisonous gas was unknown when rescue efforts commenced, firefighters were included among the victims.

On February 6, 2004, a terrorist bomb exploded in the Moscow subway. A train passing through the tunnel between Avtozavodskaya and Paveletskaya stations was attacked 400 m from Avtozavodskaya station. Units from the Ministry of Internal Affairs, the Federal Security Service, and the Ministry of Emergency Situations were directed to the scene. Because the rail car was badly damaged, rescue efforts were complicated. The death toll was 39, and 122 were injured.

Subway Tunnel Fires

When fire occurs in a rail car undercarriage or hardware compartment, the concentration of combustion products in the car may reach the danger level 3–5 minutes after ignition. Temperatures outside the car at the level of 1.5 m from the tunnel floor may reach 200 °C in 6–8 minutes after ignition. After 5–15 minutes, the fire can reach the passenger compartment. In 5–10 minutes, the fire can spread through the whole car, and temperatures inside it can reach 900–1,000 °C. The spread of the fire inside the car does not depend on tunnel air velocity and can have a rate of 1.5 m/minute. Flame spreads through the entire train at the same velocity.

After the fire has spread to one or two cars, combustion is regulated by air supply, and the total time that the train can burn can range from 3 to 7 hours. Smoke spreads through the ventilation air stream and even against it, when air velocity is less than 1.5 m/second. The fire can be approached from the fresh air side if air velocity is at least 0.75 m/second. In that case, the temperature at

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

positions where firefighters might be positioned (at a level of 1.5 m from the tunnel floor) does not exceed 70 °C. An illustration of temperature gradients at the fire location is shown in Figure 13.

Results of temperature modeling of a free-developing fire in a six-car train in a tunnel are shown in Figure 14. These calculations were based on the results of large-scale fire experiments conducted on a real train car in an experimental tunnel. Temperature dynamics in points between the cars is presented in the diagram.

Figure 14 shows that the temperature of the gas flow increases in the direction of fire propagation and reaches its maximum on the edge of the flame zone. The amplitude of the maximums rises asymptotically with the number of burning cars. The most intense temperature dynamic is realized at the end of the train.

The experimental studies of hazard factor dynamics during fires in the rail operator's compartment and in undercarriage machinery were carried out on real cars in an experimental tunnel. A fan ventilation apparatus was installed at one end of the tunnel to maintain airflow velocity at 1.5 m/second. The area of the fire was limited by the envelope of the operator's compartment. It was determined by analysis of temperature and carbon oxide concentration readings that passengers may be evacuated from the carriage if the combustible load does not exceed 45 kg/m^2.

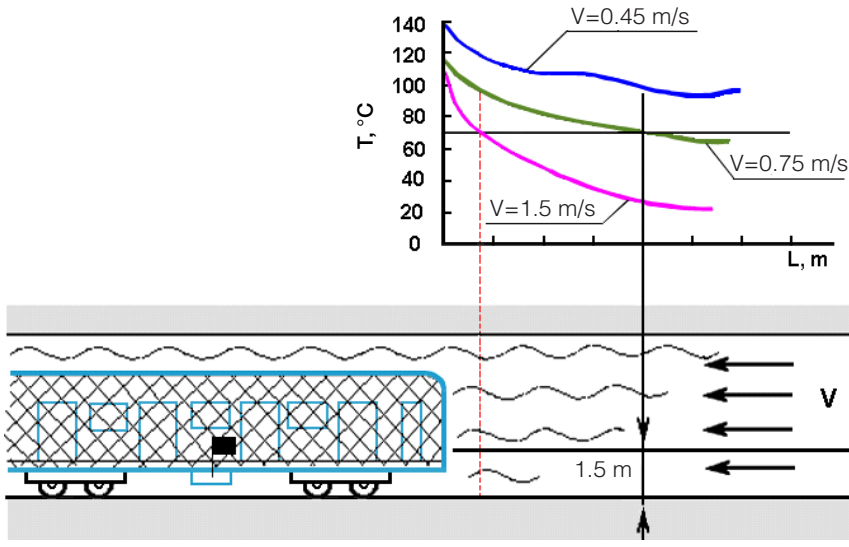


FIGURE 13 Temperature in the vicinity of the burning train car.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

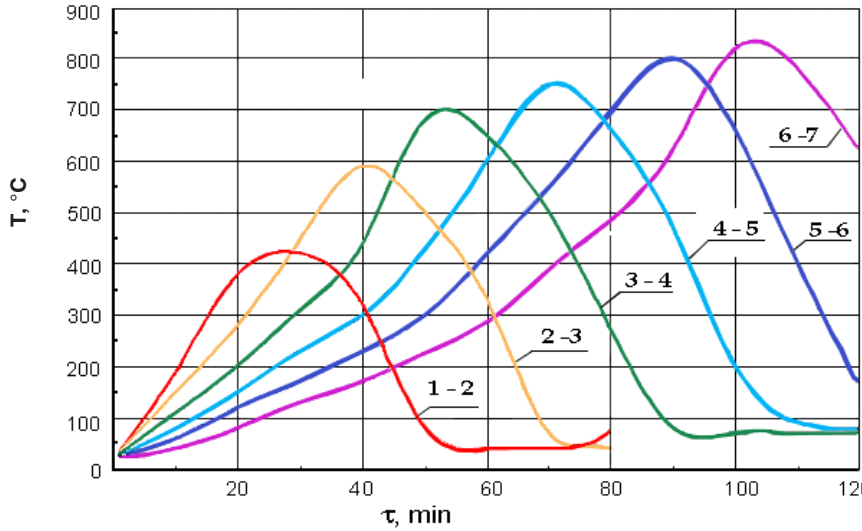


FIGURE 14 Temperature regime of a burning subway train.

Subway Station Fires

When a train is burning at a station, the fire propagates at a rate of 1–1.5 m/second. Smoke concentrations reach dangerous levels in 7–12 minutes, which allows enough time to evacuate people during rush hour. If the emergency ventilation system is not switched on immediately or is ineffective, smoke obscures the evacuation exits within 1–2 minutes. Combustible materials may also ignite on the platform at which the burning train is standing. The temperature at points removed from the burning train (on the opposite platform, at the escalator) increases slowly and reaches dangerous levels only 10–25 minutes after the start of the fire (see Figure 15).

EVACUATION FROM BUILDINGS

Analysis of the consequences of fires in buildings with large numbers of people inside indicates that simply meeting the requirements of architectural standards does not guarantee people's safety if a fire occurs. The high-density traffic flows with large numbers of participants that fires create are almost as dangerous as the fire itself. Thus, organizing evacuation remains a problem of utmost importance for all types of multistory residential and commercial buildings.

Evacuation should be organized not only to remove people from a danger zone in a timely manner but also to avoid long-lasting accumulations of people on evacuation routes. The problem can be resolved by employing fire alarm and

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

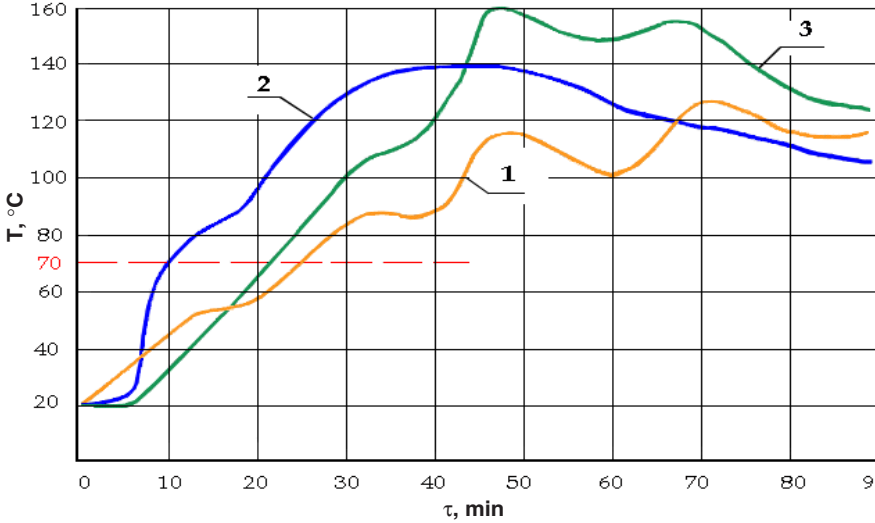


FIGURE 15 Temperature of the subway station during rolling stock fire.
Note: **1**—at escalator entrance if fire originated in the middle of the train; **2**—the same if fire originated in the car nearest to the escalator; **3**—on the opposite platform if fire originated in the middle of the train.

evacuation control systems. Such systems should be designed using results of the analysis of possible fire scenarios.

There are a sufficient number of methods for estimating necessary evacuation parameters. In Galea and others' article on evacuation of the World Trade Center, the authors attempted to model the process of evacuation from a 100-story building in different situations.[4]

The first model describes a situation in which there are 7,000 people in the building. The people are distributed evenly on all floors of the building, so there are 70 persons on each floor. Evacuation is carried out using three staircases: through L1, 3,000 people; through L2, 2,000 people; and through L3, 2,000 people.

Evacuation time in this first model equals 24.4 minutes. The results of the calculations indicate that the critical values for the accumulation of people in the evacuation routes are not achieved. Human accumulation curves have a discontinuous character, because every person entering and leaving a particular area

[4]Galea, E. R., P. Lawrence, S. Blake, S. Gwynne, and H. Westeng. 2004. A Preliminary Investigation of Evacuation of the WTC North Tower Using Computer Simulation. In Human Behavior in Fire. Proceedings of the 3rd International Symposium. Belfast: Interscience Communications Ltd.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

changes the accumulation value for a value divisible by the area of its projection on the floor. Therefore, when the quantity of people in the building is much less than the maximum, evacuation time depends on the length of the evacuation routes.

In the second model, it was assumed that two of the staircases are blocked at the 91st floor. All people from the 91st floor are evacuated by one staircase to the 90th floor. There are 70 people on each floor, so there are 700 people in total on floors 91 to 100. The staircase was assumed to be 1.4 m wide. After the calculations were made, the staircase width was increased up to 2 m and the calculations were repeated.

The estimated time to evacuate people from the 100th floor to the 90th floor through the 1.4 m-wide staircase equals 7.2 minutes. The estimated time for the same evacuation through the 2 m-wide staircase is 3.1 minutes.

It is shown that for the 1.4 m-wide staircase, critical values for the accumulation of people are achieved in the first minutes of the evacuation and are maintained throughout the process. For the 2 m-wide staircase, the estimated evacuation time is one-half that for the narrower staircase and the accumulation value throughout the process is less than critical. Thus estimated evacuation time depends to a great extent on the width of exit pathways.

In the third model, it was also assumed that two of the staircases are blocked at the 91st floor. All people from the 91st floor are evacuated by staircase to the 90th floor. The third model is the same as the second except that it is assumed there are 220 people on each floor, so there are 2,200 people in total on floors 91 to 100. The calculations were made for the two staircase widths, 1.4 m and 2 m.

The estimated time to evacuate people from the 100th floor to the 90th floor through the 1.4 m-wide staircase equals 23.1 minutes. The estimated time for the same evacuation through the 2 m-wide staircase equals 15.7 minutes.

It is shown that the width of the evacuation pathway is the most important factor affecting estimated evacuation time. For the third model for the 1.4 m-wide staircase, critical values for the accumulation of people in the evacuation routes are achieved in the first minute of the evacuation and are maintained until the end of the process. For the 2 m-wide staircase, the estimated evacuation time is approximately 75 percent of that for the narrower staircase, but the accumulation value is still more than critical.

Evacuation time may be reduced by using special rescue equipment. For example, elastic tube evacuation systems are the most promising and effective means for this purpose and are widely used throughout the world. An evacuation tube works by using frictional force to reduce the velocity of the descending body inside the tube. Descent velocity depends on tube construction and may be regulated by the evacuated person by moving his or her limbs and by rescue workers on the ground manipulating the tube. An evacuation tube consists of several coaxial cylindrical fabric layers. Each layer has its own function. The nonstretch layer works as the bearing element and resists longitudinal tensions.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

The elastic layer embraces the descending person with the necessary force. The external layer resists fire.

Evacuation tube systems have several advantages:

- They may be used to evacuate people from heights of up to 100 m.
- They operate independent of weather conditions, climate, or time of the day.
- They are capable of passing up to 30 people per minute.
- They do not require time for activation or special training for their use.
- They provide evacuation for every person regardless of physical and mental condition.
- They help evacuees overcome the fear of heights.

An evacuation tube may be installed inside or outside the building, may be entered from one or several floors, may be carried by firefighters to the scene, or may be installed on turntable ladders.

FIREFIGHTING UNDER TERRORIST FIRE

Firefighting tactics in combat conditions have not yet been developed. To understand the problem, it is useful to study the terrorist attack on the Beslan elementary school as an example.

At 9:00 a.m. on September 1, 2004, the North Ossetia-Alania office of the Ministry of Emergency Situations received word of a terrorist attack on Beslan's Elementary School Number 1. In addition to combat units, two AZ-40 fire trucks from the Beslan fire department were directed to the scene. The units were deployed in the area around the school by the mobile command center.

At 1:05 p.m., rescue workers from Centrospas (State Central Aero-Mobile Rescue Brigade) received orders to remove bodies from the school building. With the terrorists' permission, rescue vehicles approached the school and rescue workers entered the building to begin work. A few minutes later, two explosions occurred in the school gymnasium, which caused a roof collapse and partial wall destruction followed by fire. The hostages began to panic. Some of them tried to escape, and the terrorists began shooting at them. The action phase of the operation had begun.

Combat continued until 3:00 p.m., when the necessary safety level for the firefighters to start work was achieved and the order to begin extinguishing the fire was received. Reconnaissance showed the area of the fire to be approximately 800 m^2, and the nearest fire hydrants were within the terrorists' firing range.

The fire department officer in charge decided to employ two hoses supplied by a fire truck water tank, using nearby buildings and structures as cover. At 3:30 p.m., two more fire trucks arrived from the State Fire Service group of the

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Ministry of Emergency Situations. A mobile firefighting command center was established at the scene, and two firefighting units were formed to put RS-50 and RS-70 hoses through doorways, windows, and wall breaches. The hoses were supplied by water carried to the spot in turns by fire truck water tanks.

After two more fire vehicles from the special fire brigade of Vladikavkaz and a fire truck from the Ardon fire brigade arrived, a hose line was laid out to supply water from a distant hydrant located in a safe zone. It allowed firefighters to engage two more RS-70 hoses, which brought the fire under containment by 3:34 p.m.; three RS-70 and two RS-50 hoses were used.

At 6:30 p.m., firefighters were moved out of the area of possible crossfire by order of the commander of the Alpha special tactical unit. When shooting from the south part of the building ceased, firefighters resumed their efforts to extinguish the fire. At 9:09 p.m., the fire was out, but hoses continued to be used to provide cover for rescue operations.

At 12:05 a.m., information was received regarding a fire in the destroyed south part of the school building. The fire was caused by bomb explosions that destroyed the loft and floor slabs. Two RS-50 hoses supplied by fire truck water tanks were engaged in extinguishing flames in piles of wreckage on the ground floor and the partially destroyed first floor. Later the hoses were connected to the water-supplying hose line. The fire was contained at 12:32 a.m. and put out at 3:10 a.m. At 7:00 a.m., after reconnaissance was completed, rescue workers from the Ministry of Emergency Situations began combing through the piles of wreckage looking for bodies. Rescue operations ended at 7:00 p.m.

The fire was not interesting from the standpoint of firefighting tactics. Firefighting personnel and equipment concentrated on the scene were sufficient to put out the fire at any moment. However, firefighting operations were hindered by a lack of combat defensive equipment and armor for firefighters and fire vehicles. Two rescue workers were killed and two were wounded, and three firefighters received contusions.

One way to solve the problems of firefighting in combat zones is to develop firefighting robotics technology. Such technology may also be useful for firefighting in conditions of chemical or radioactive contamination. Development of such technologies is already under way in Russia.

Copyright National Academy of Sciences. All rights reserved.

A Decision Informatics Approach to Urban Emergency Management

James M. Tien
Rensselaer Polytechnic Institute

INTRODUCTION

Urban infrastructures are the focus of terrorist acts because, quite simply, they produce the most visible impact, if not casualties. From the September 11, 2001, attack on New York City's World Trade Center to the more recent March 11, 2004, attack on Madrid's commuter trains, it is obvious that urban centers are indeed vulnerable to such hideous acts. While terrorist acts are the most insidious and onerous of all disruptions, there are many similarities to the way one should deal with these willful acts—which would also include a malicious prankster releasing an electronic virus on the Internet—and those caused by natural and accidental incidents that have also resulted in adverse and severe consequences. However, there is one major and critical difference between terrorist acts and the other man-made but accidental disruptions: the terrorist acts are willful, and therefore also adaptive. Since terrorist and other willful acts (for example, electronic viruses, hacker attacks, and e-mail spam) are based on the most up-to-date intelligence or information, one must also counter these acts with the same, if not more sophisticated, willful, adaptive, and informed approach.

More specifically, the approach of real-time, information-based decision making, which Tien (2003) has called the decision informatics paradigm, is focused on decisions and based on multiple data sources, data fusion and analysis methods, timely information, stochastic decision models, and a systems engineering outlook. It should be emphatically stated that while the terms employed in describing the methodologies that underpin decision informatics are those belonging to decision analysis (emergency management, statistics, risk analysis,

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

and so forth), decision informatics is clearly multidisciplinary in nature and, depending on the problem being considered, could include experts from science (information, cognition, sociology, and so forth), engineering (telecommunications, biomedical, chemical, and so forth) and other disciplines (religion, terrorism, culture). It provides a systematic and consistent way to address real-time emergency issues, including those concerned with the preparation for a major disruption, the prediction of such a disruption, the prevention or mitigation of the disruption, the detection of the disruption, the response to the disruption, and the recovery steps that are necessary to adequately, if not fully, recuperate from the disruption. More importantly, one must approach an urban emergency management problem in a systemic or holistic manner, especially given the interdependencies of the underlying infrastructure systems.

Although the focus of this paper is primarily on terrorist disruptions, it is obvious that the decision informatics approach is likewise applicable to the preparation, prediction, prevention, detection, response, and recovery steps associated with the emergency management of any major urban disruption. The remaining sections of this paper deal with the types of disruption, the stages of or life cycle in a disruption, the decision informatics paradigm, and the combination of types, stages, and decisions in the efforts of the Department of Homeland Security (DHS) and its academically based Homeland Security Centers of Excellence, followed by some concluding remarks.

TYPES OF DISRUPTIONS

Modern society relies on the reliable operation of a set of human-built systems—each being a combination of people, processes, goods, services, physical structures, and institutions—to sustain people themselves, infrastructures, and commerce. In the United States, the constructed systems—most of which are privately owned and operated—are so essential that they have been called the nation's lifelines. They are included in the broader set of critical infrastructures defined by the President's Council on Critical Infrastructure Protection (PCCIP) (U.S. President, 2001) to be those physical and cyber-based systems essential to the minimum operations of both the economy and the government.

Historically, the nation's critical infrastructures have been physically and logically separate systems that had little interdependence. However, as a result of advances in information technology and the necessity for improved efficiency and effectiveness, these infrastructures have become increasingly automated and interlinked. In fact, because the information technology revolution has changed the way business is transacted, government is operated, and national defense is conducted, the U.S. President (2001) singled it out as the most critical infrastructure to protect following September 11, 2001. Thus, while the United States is considered a superpower because of its military strength and economic prowess, nontraditional attacks on its interdependent and cyber-supported infrastructures could significantly harm both the nation's military power and economy. Clearly,

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

infrastructures, especially the information infrastructure, are among the nation's weakest links; they are vulnerable to willful acts of sabotage. The NRC Committee on the Role of Information Technology in Responding to Terrorism (2003) has made a number of recommendations to reduce vulnerabilities associated with the information infrastructure, including undertaking more research in authentication, detection, containment, and recovery.

The infrastructure interdependencies are most obvious when a disruption occurs. For example, interruptions in power and communications following the September 11, 2001, attack, in turn, forced the closing of the New York Stock Exchange, which is a critical part of the nation's banking and finance infrastructure. As another example, the August 2003 electrical power outage on the East Coast caused the failure of wireless communications and affected the city of Cleveland's water system. Clearly, there are innumerable interdependencies among the various infrastructure networks or systems that provide for a continual flow of goods and services essential to the defense and economic security of a nation. Indeed, for this reason, it is inappropriate to only categorize some infrastructure systems as being critical; they are all critical to the proper functioning of a nation or urban center; otherwise, the noncritical ones might well become the weakest links and thus vulnerable to attack and destruction. More importantly, the infrastructure interdependence problems should not be minimized, especially from a security and reliability perspective. In fact, contingency plans or backup systems should be developed and employed to mitigate these problems.

Sadly, the same advances that have enhanced interconnectedness have created new vulnerabilities, especially related to equipment failure, human error, weather, and other natural causes, and physical and cyberattacks. Thus electronic viruses, biological agents, and other toxic materials can turn a nation's lifelines into deathlines, in that they can be used to facilitate the spread of these materials, whether by accident or by willful act. Even the Internet—with almost a billion users—has become a terrorist tool; jihad Web sites are recruiting members, soliciting funds, and promoting violence (for example, by showing the beheading of hostages). Also, as evidenced by the September 11, 2001, attack, components of an infrastructure system can be used as weapons of destruction.

As identified earlier, there are, in essence, three types of disruptions: natural incidents due to nature or natural forces, accidental incidents due to human errors or structural failures, and willful incidents due to human acts or destructive weapons. The who, what, when, and where of a number of well-known disruptions occurring in the latter half of the twentieth century are considered in Table 1.

The question remains: Are there differences between natural, accidental, and willful disruptions? The answer is an emphatic yes; indeed, these differences point to the need for a more adaptive, informed, and decision-oriented approach for dealing with willful acts than for reacting to natural and accidental disasters.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 1 Example Disruptions

	Nature of Disruption
Description	Who?
Natural	
1969 Hurricane Camille	Hurricane Camille was a category 5 (out of a possible 5) hurricane.
2002 SARS (Severe Acute Respiratory Syndrome) epidemic	Employing DNA sequencing information, SARS was identified in 24 hours as a coronavirus strain from wild animals, including poultry.
2004 South Asia Tsunami	A magnitude 9.0 Indian Ocean earthquake caused tsunami tidal waves of up to 50 feet.
Accidental	
1984 Bhopal Gas Tragedy	Toxic methylisocyanate chemical vapor escaped from the Union Carbide plant due to safety valve malfunction.
1986 Chernobyl Nuclear Disaster	While testing Reactor 4 and ignoring safety procedures, a chain reaction caused explosion and release of highly radioactive material.
1989 United 232 Explosion	Failure of all three hydraulic flight control systems of Northwest's DC-10 caused the crew to almost completely lose control of the aircraft.
Willful	
1993 Oklahoma City Bombing	Timothy McVeigh and others built bomb that was placed in a rented Ryder truck.
1995 Tokyo Subway Sarin Attack	Members of a terrorist group attacked five subway lines leading to the center city with toxic sarin nerve gas.
September 11, 2001, Tragedy	Nineteen terrorists hijacked four airliners, each loaded with thousands of gallons of jet fuel, and crashed them into highly visible U.S. targets.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

When?	What?	Where?
August 17, 1969, 2 a.m.	Regional: 255 killed; thousands evacuated; $4.2 billion in damages	Makes landfall along Mississippi coastline
November 2002–July 2003	Worldwide: 774 killed; 7,322 injured	Began in South China, then Canada and Southeast Asia and a few cases in Europe and the United States
December 26, 2004, 8 a.m.	Regional: more than 160 thousand killed; thousands injured; millions displaced	Affecting Indonesia, Sri Lanka, India, and Thailand
December 2, 1984, 11 p.m.	Regional: more than 10 thousand killed; more than 0.5 million injured	Small town of Bhopal, India
April 26, 1986, 1 a.m.	Regional: 31 immediately killed; thousands injured and suffering disease; millions affected by remaining radiation	Chernobyl nuclear power plant consisting of four reactors located in Ukraine
July 19, 1989, 3 p.m.	Local: 186 (of 300) crew and passengers killed; many injured	Plane crash-lands on runway in Sioux City, Iowa
April 19, 1993, 9 a.m	Local: 168 killed; hundreds injured; building destroyed	Oklahoma City Alfred P. Murrah Federal Building
March 20, 1995, 8 a.m.	Local: 12 killed; thousands injured	Subway cars in Tokyo, Japan
September 11, 2001, 8:47 a.m.–10:06 a.m.	Local: 3,000 killed; billions of dollars of infrastructure and commercial damage	American Airlines flight 11 crashes into World Trade Center (WTC) north tower; United Airlines flight 175 crashes into WTC south tower; American Airlines flight 77 crashes into Pentagon; United Airlines flight 93 crashes in field near Shanksville, Pennsylvania

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

More specifically, Table 2 considers the different types of disruptions from four perspectives: cause, onset, target, and impact.

STAGES IN A DISRUPTION

The mission and overriding objective of the U.S. Federal Emergency Management Agency (FEMA), which is now a part of DHS (U.S. Congress, House, 2002), is to help the nation be ready to respond to disasters and disruptions of all kinds through a comprehensive, risk-based emergency preparedness program.

Traditionally, FEMA's comprehensive emergency management system is composed of four stages: preparedness, mitigation, emergency response, and recovery. From a decision perspective, it is helpful to consider an expanded, six-stage process: preparation (corresponding to preparedness), prediction, prevention (corresponding to mitigation), detection, response (corresponding to emergency response), and recovery (corresponding to recovery). The additional prediction stage is necessary because it is beyond general preparation and helps focus prevention tactics; it requires a set of methodologies and technologies that is statistical in nature and risk-based in approach. The additional detection stage is also necessary; it follows prediction and precedes response and is very much dependent on data obtained from multiple data sources or sensors and the careful fusion and analysis of that data. Table 3 identifies the six stages of a disruption's life cycle in terms of related decisions that must be considered at each stage.

DECISION INFORMATICS

In critically reviewing the disruption characteristics and related decisions identified in Tables 2 and 3, respectively, it is obvious that real-time, information-based decision making is needed for addressing major disruptions, especially terrorist acts, which are quite adaptive in reality. Alternately, what is needed is a decision informatics paradigm, as depicted in Figure 1. That is, the nature of the required real-time decision (in connection with each of the six stages of a disruption) determines, where appropriate and from a systems engineering perspective, the data to be collected (possibly, from multiple, nonhomogeneous sources) and the real-time fusion and analysis to be undertaken to obtain the needed information for input to the modeling effort, which in turn provides the knowledge to support a timely decision. The feedback loops in Figure 1 are within the context of systems engineering; they serve to refine the analysis and modeling steps.

Thus decision informatics concerns three related issues, that is, decisions, data, and information, and is underpinned by three multidisciplines, that is, data fusion and analysis, decision modeling, and systems engineering. In abbreviated form there are six steps in the decision informatics process: decisions, data,

Copyright National Academy of Sciences. All rights reserved.

TABLE 2 Disruption Characteristics

		Types of Disruption		
	Characteristics	Natural	Accidental	Willful
Cause	Primary	Nature	Human Errors	Human Acts
	Secondary	Natural Forces	Structural Failures	Destructive Weapons
Onset	Period	Hours/Days	Hours	Minutes
	Predictability	High	Medium	Low
	Adaptability	Low	Low	High
Target	Primary	Infrastructures	Infrastructures	People
	Secondary	Commerce/People	Commerce/People	Infrastructures/Commerce
	Vulnerability	Indiscriminate	Indiscriminate	Weakest Link
Impact	Spatial	Regional/Worldwide	Local/Regional	Local
	Temporal	Years	Months/Years	Months/Years
	Damage	Medium/Large	Medium/Large	Medium/Large

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 3 Life Cycle of a Disruption: Stages and Related Decisions

Stages	Related Decisions
Preparation	How and where do terrorist groups form and recruit? How are targets picked and what motivates a willful act? How can potential terrorists be converted away from terrorism? How can one prepare for disruption without degrading quality of life and civil liberties? How can one integrate the help of industry and other private organizations? What type of resources (for example, protective gear) are available and at what locations? What integrated emergency command center needs to be established? How can one coordinate and standardize data, medical records, information systems, and communications? Is the preparation appropriate for both security and safety? How can one effectively assess preparedness?
Prediction	What precursor signals can be associated with natural, accidental, and willful incidents? What is the nature (for example, self-assembled, self-replicated) and scope of such attacks? What facilities, assets, and resources are most vulnerable to attack? In addition to direct threats, what are possible indirect or secondary threats (for example, zoonotic diseases, hurricane-related freshwater flooding)? How best can one pre-position resources for the most likely and most risky disruptions? How can one communicate accuracy of prediction? How can one provide education and simulated training for decision makers and responders?
Prevention	What identification (for example, biometric) technologies can be reliably employed to prevent unlawful entry? How can one prevent attacks, reduce vulnerability, minimize damage, and enhance recovery? How can one develop contingency plans or backup systems to mitigate interdependency problems? How can one warn the public (for example, color-coded alerts, terrorist threat index)? How and when is it possible to mitigate (for example, evacuate) before the disruption? How is it possible to mitigate problems of communications, traffic gridlock, and interjurisdictional issues? How is it possible to prevent problems associated with the roles and responsibilities of all involved? Are the prevention strategies sustainable and are they commensurate with the risk level?

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 3 *Continued*

Stages	Related Decisions
Detection	What sensors can be employed to detect a disruption? How is it possible to fuse and abstract valid and useful information from multiple data sources? What response preparation should be effected (for example, level of emergency)? How is it possible to validly identify the nature of an attack? What is the target (including people, infrastructures, and commerce) and scope (including time, space, and weapon used) of the attack? How is it possible to mitigate the potential impact of an attack? How is it possible to strengthen the public's resilience to the disruption?
Response	Where should an emergency staging and medical triaging center be established? How is it possible to logistically inventory and disburse available resources, requested resources, and donated goods? How is it possible to coordinate and secure communications by computer, cellular, radio, and telephone lines? How is it possible to reposition resources for another attack or response to other incidents? How is it possible to coordinate and integrate workers and volunteers? How is it possible to coordinate within and between response levels (that is, local, regional, state, and federal)? How is it possible to communicate with the public, including dealing with the media?
Recovery	Which targets remain at risk and must be taken out of harm's way? What can be done to recover from the resultant damages? How is it possible to store, protect, retrieve, and recover critical data? What state, federal, and commercial aid can be obtained to fund the recovery? What recovery goals, measures, and assessment procedures have been established? What projects, tasks, budget, and schedule are necessary for the recovery? What can be put in place to forestall or prepare for another disruption?

analysis, information, models, and systems. These steps are summarized in Table 4.

Finally, it should be noted that decision informatics is, as a framework, generic and applicable to most, if not all, decision problems. Further, since any data analysis or modeling effort should only be undertaken for some purpose or decision, all analyses and modeling activities should be able to be viewed within the decision informatics framework. In short, decision informatics represents a decision-driven, information-based, adaptive, real-time, human-centered, inte-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

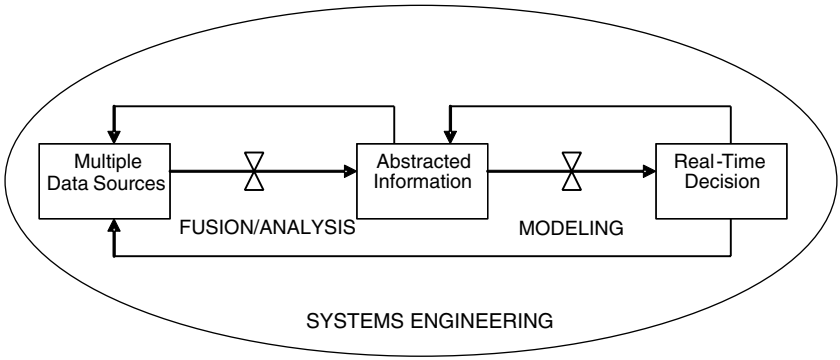


FIGURE 1 Decision informatics paradigm.

grated, and computationally intensive approach to intelligent decision making by humans or software agents. Consequently, it can be very appropriately employed to address decisions at the preparation, prediction, prevention, detection, response, and recovery stages of an urban disruption.

HOMELAND SECURITY

Following the September 11, 2001, attack on the U.S. homeland, the U.S. Homeland Security Act of 2002 (Public Law 107-296, see U.S. Congress, House, 2002) was immediately passed; it established DHS with a mission to "a) prevent terrorist attacks within the United States; b) reduce the vulnerability of the United States to terrorism; and c) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States." Additionally a number of high-level reports have been published on how to make the homeland more secure from future acts of terrorism. The U.S. National Academies formed the Committee on Science and Technology for Countering Terrorism (2002); it strongly urged, among several other important recommendations, a risk- or decision-based approach to measuring and countering terrorism. It also helped define the Directorate of Science and Technology that is now a part of DHS. More recently, the National Commission on Terrorist Attacks Upon the United States (2004) is recommending the establishment of a National Counterterrorism Center—with a National Intelligence Director—to unify all counterterrorism intelligence and operations across the foreign-domestic divide in one organization. This and other commission recommendations are currently being addressed in Congress.

As stated in two related presidential directives (U.S. President, 2003a,b), the National Response Plan (NRP) (DHS, 2004) establishes a comprehensive all-hazards approach to enhance the ability of the nation to manage domestic inci-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 4 Decision Informatics Steps

Steps	Considerations
Decisions	
Disruptions	Natural, Accidental, Willful
Levels	Operational, Tactical, Strategic, Systemic
Targets	People, Infrastructures, Commerce
Data	
Attributes	Measurability, Availability, Consistency, Validity, Reliability, Stability, Accuracy, Independence, Robustness, Completeness
Sources	Sensors Intelligence (SENSINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Human Intelligence (HUMINT)
Issues	Standards, Compatibility, Interoperability, Scale
Analysis	
Types	Data Fusion, Data Analysis, Data Mining, Data Interpolation, Evolutionary Algorithms, Strengths, Weaknesses, Opportunities, Threats
Disciplines	Decision Analysis (Statistics, Risk Analysis, Operations Research, Economics), Science (Information, Cognition, Psychology, Sociology, Behavior, Organization, Computer, Agriculture, Livestock, Food, Ocean, Atmosphere), Engineering (Telecommunications, Human Factors, Biomedical, Chemical, Nuclear), Other (Religion, Terrorism, Culture)
Information	
Attributes	Same as Data Attributes
Sources	Same as Data Sources
Types	Threats, Vulnerabilities, Risks, Damages (Mortality, Morbidity, Physical, Environmental, Financial)
Issues	Same as Data Issues
Characteristics	Processed Data, Derivations, Groupings, Patterns
Models	
Types	Descriptive (System Dynamics, Simulation), Prescriptive (Mathematical Programming, Dynamic Programming), Adaptive (Evolutionary Models, Bayesian Networks)
Disciplines	Same as Analysis Disciplines
Systems	
Attributes	Intra-/Interdependent, Natural/Human-made, Physical/Conceptual, Static/Dynamic, Closed/Open
Resources	Law Enforcement, Firefighting, Public Works, Public Health, Emergency Medical, Private, Financial
Networks	Private (Organizations, Institutions), Public (Local, Regional, State, Federal), Cyber
Issues	Privacy, Civil Liberties, Quality of Life

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

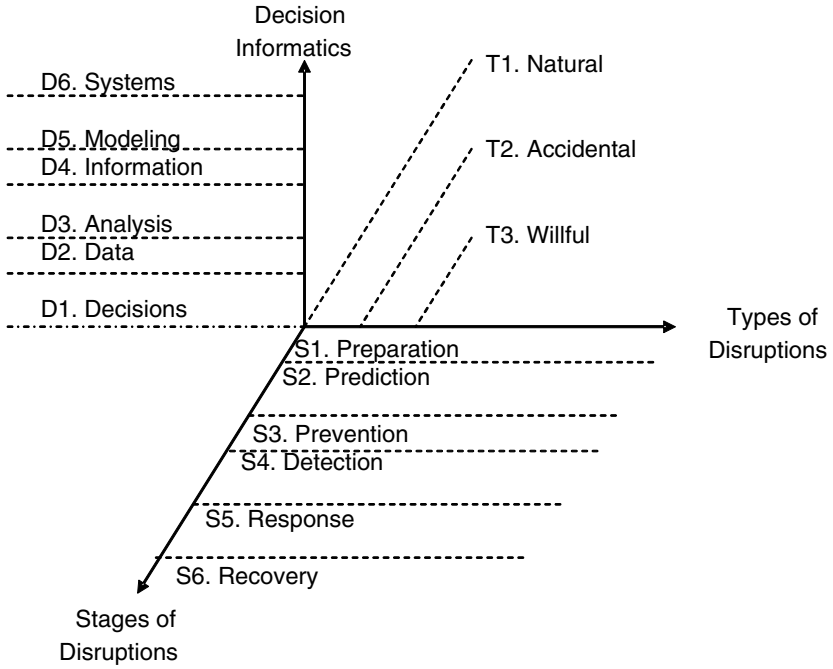


FIGURE 2 Urban disruptions: types, stages, and decisions.

dents. The NRP incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of the federal government's coordination with state, local, and tribal governments and the private sector during incidents. Further, to enhance the ability of the nation to manage domestic incidents, a single, comprehensive National Incident Management System (NIMS) is being established. The NRP is predicated on the NIMS. Together, the NRP and the NIMS provide a nationwide template for working together to prevent or respond to threats and incidents regardless of cause, size, or complexity.

DHS is organized into four major directorates: Border and Transportation Security (including sensors, signals, passenger profiling, and prevention tactics), Emergency Preparedness and Response (including preparation, prediction, prevention, detection, response, and recovery), Information Analysis and Infrastructure Protection (including data fusion and analysis, disruption modeling, performance versus cost analysis, vulnerability/risk assessment tools, and systems considerations), and Science and Technology (including biometric sys-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

tems, weapons detection systems, and satellite image systems). DHS actually outsources many of its activities through contracts and grants—to federal laboratories, government agencies, and private organizations. In April 2004 the $130 million, 4.5-year Homeland Security Institute was established at Analytic Services, Inc., or ANSER, a systems engineering think tank modeled after the RAND Corporation.

Additionally, through the Office of University Programs within the Science and Technology Directorate, DHS is engaging the academic community to create learning and research environments in areas critical to homeland security. Labeled Homeland Security Centers of Excellence, it is helpful to consider them within the three-dimensional framework—types, stages, and decisions—discussed in the previous sections of this paper. As depicted in Figure 2, this framework identifies 3 by 6 by 6, or 108, possible foci for study consideration. Thus far, four Homeland Security Centers of Excellence have been established, while a fifth one is forthcoming; they are summarized in Table 5.

CONCLUDING REMARKS

Securing the homeland from damaging willful acts is a matter of trade-offs: between security and people, in particular, people's privacy, civil liberties, and quality of life; between security and infrastructures, in particular, infrastructures that are highly interdependent; and between security and commerce, in particular, commerce that is dependent on highly efficient and nonredundant processes. In short, it is a trade-off between security and a free society.

Interestingly, the tools or technologies that underpin a modern society are likewise the weapons that can be used to undermine, if not destroy, society. Biological, chemical, and nuclear breakthroughs can also be considered to be weapons of mass destruction; the highly effective Internet provides a medium for cyberviruses, hackers, and spammers; and airplanes are employed as missiles against people, infrastructures, and commerce.

The decision informatics approach to urban emergency management can clearly address a number of vulnerabilities, including natural disasters, accidental tragedies, and willful acts. Several comments should be made about this approach. First, it is multidisciplinary in nature; obviously, depending on the problem being considered, it requires experts from many disciplines. Second, it is evolutionary in practice; as a problem becomes better understood, the approach could be better refined and made more expeditious. Third, it is systemic in scope; it seeks to consider a problem from different perspectives, in terms of, for example, efficiency and reliability, public and private goals, and domestic and international concerns.

The purpose of this paper, then, is to argue for the development of decision technologies that can be employed to prepare for a major disruption, if not predict and possibly prevent the disruption. Such technologies should also detect

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 5 Homeland Security Centers of Excellence: Focus on Types, Stages, and Decisions

Established (3-Year Funding)	Lead/Primary Partner Universities/Others	Scope
November 2003 ($12 million)	**Univ. of Southern California** Univ. of Wisconsin, Madison New York Univ. North Carolina State Univ. Carnegie Mellon Univ. Others: Consultants, Academia	Risk analysis related to economic consequences of terrorist threats and events
April 2004 ($18 million)	**Texas A&M Univ.** Univ. of Texas/Medical Branch Univ. of California, Davis Univ. of Southern California Univ. of Maryland Others: Industry, Government, Academia	Potential threats to animal agriculture, including foot-and-mouth disease, Rift Valley fever, avian influenza, and brucellosis
April 2004 ($15 million)	**Univ. of Minnesota** Michigan State Univ. Univ. of Wisconsin, Madison North Dakota State Univ. Georgia Institute of Technology Others: Major Food Companies	Agro-security issues related to postharvest food protection
January 2005 ($12 million)	**Univ. of Maryland** Univ. of California, Los Angeles Univ. of Colorado, Boulder Monterey Institute of International Studies Univ. of Pennsylvania Univ. of South Carolina, Columbia Others: Academia	Applying social science to the understanding and prevention of terrorism
Forthcoming ($15 million)	To be determined.	Ways to prepare for, respond to, and recover from major disasters

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Center Name	Types	Stages	Decisions
Homeland Security Center for Risk and Economics Analysis of Terrorism Events (CREATE)	Willful	Preparation Prediction Prevention Response	Decisions Data Analysis Information Modeling Systems
Homeland Security National Center for Foreign Animal and Zoonotic Disease Defense	Natural Accidental Willful Detection	Preparation Prediction Prevention Response	Decisions Data Analysis Information Modeling Systems
Homeland Security Center for Food Protection and Defense	Accidental Willful	Preparation Prediction Prevention Detection Response	Decisions Data Analysis Information Modeling Systems
Homeland Security Center of Excellence on Behavioral and Social Research on Terrorism and Counterterrorism	Willful	Preparation Prediction Prevention Recovery	Decisions Data Analysis Information Modeling Systems
Homeland Security Center for the Study of High Consequence Event Preparedness and Response	Natural Accidental Willful	Preparation Prediction Prevention Detection Response Recovery	Decisions Data Analysis Information Modeling Systems

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

the disruption, identify the responses required to deal with the resultant situation, and then, following the disruption, specify the recovery steps that are necessary to satisfactorily recuperate from the disruption.

REFERENCES

National Commission on Terrorist Attacks Upon the United States. 2004. The 9/11 Commission Report. Washington, D.C.: W. W. Norton and Company.

NRC Committee on Science and Technology for Countering Terrorism. 2002. Making The Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C.: The National Academies Press.

NRC Committee on the Role of Information Technology in Responding to Terrorism. 2003. Information Technology for Counterterrorism: Immediate Actions and Future Possibilities. Washington, D.C.: The National Academies Press.

Tien, J. M. 2003. Towards a Decision Informatics Paradigm: A Real-Time, Information-based Approach to Decision Making. IEEE Transactions on Systems, Man, and Cybernetics, Special Issue, Part C, 33(1):102–113.

U.S. Department of Homeland Security (DHS). 2004. National Response Plan. Washington, D.C.: Department of Homeland Security.

U.S. Congress, House. 2002. Homeland Security Act of 2002. Public Law 107-296, as amended. H. R. 5005-8. 107th session.

U.S. President. 2001. Executive Order on Critical Infrastructure Protection. Washington, D.C.: The White House, October 16.

U.S. President. 2003a. Homeland Security Presidential Directive (HSPD) 5. Washington, D.C.: The White House, February 28.

U.S. President. 2003b. Homeland Security Presidential Directive (HSPD) 8. Washington, D.C.: The White House, December 17.

Copyright National Academy of Sciences. All rights reserved.

Efforts of Russian Ministries in Implementing Measures to Prevent Acts of Terrorism

Sergey G. Vasin
Department of Security and Counterterrorism,
Russian Ministry of Industry and Energy

The ministries and agencies of the Russian Federation interact with one another in accordance with existing legislation of the Russian Federation within the framework of the counterterrorism system that has been created in the country. This system is understood as the entirety of entities involved in fighting terrorism in accordance with their competencies, as well as the tasks and goals assigned to them.

Three fundamental concepts are used in this report:

1. entities for fighting terrorism—specially empowered agencies of state power, including security and internal affairs agencies, units of the Ministry of Defense, and the Russian Federal Protective Service
2. entities for countering terrorism—federal agencies of state power, executive branch agencies of Russian Federation members, local self-government bodies, organizations, and public associations involved to the extent of their competency in efforts to counter terrorism
3. forces and means of the system for countering terrorism—specially trained forces and means of federal executive-branch agencies, executive-branch agencies of Russian Federation members, local self-government bodies, organizations, and public associations intended and assigned for preventing, suppressing, and eliminating the consequences of crisis situations associated with terrorist manifestations and other extreme situations of a criminal nature

The fight against terrorism in the Russian Federation and the counteraction of its manifestations is based on the following fundamental principles:

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- provision and protection of basic human and civil rights and freedoms
- legality
- certainty of punishment for the commission of terrorist acts
- unitary leadership of forces and means involved in conducting counterterrorist operations and responsibility for their results
- priority of measures for preventing terrorism
- comprehensive use of prophylactic, legal, political, socioeconomic, and public information measures
- priority of protection for individuals placed in danger as a result of a terrorist act
- combination of open and secret methods for countering and combating terrorism
- minimal concessions to terrorists
- minimal publicity for technical methods and tactics for conducting counterterrorist operations
- ensurance that measures for countering and combating terrorism are in accordance with international law
- facilitation of the rights of the public and citizens to broad participation in efforts to counter terrorism in the form of preventing and suppressing terrorist manifestations

The legal basis for antiterrorist activities in Russia and for the interaction of ministries and agencies (in the federal executive branch) lies in the Constitution of the Russian Federation; specific federal laws, including On Combating Terrorism, On the Police, On Extraordinary Powers, On Security, On Operational Investigations Activities, On Countering the Legalization of Profits Obtained by Criminal Means and Used to Finance Terrorism (Money Laundering), On State Protection, On the Internal Troops of the Ministry of Internal Affairs of the Russian Federation, On the State Protection of Judges and Officials of Law Enforcement and Control Agencies, On Private Detective and Security Activities in the Russian Federation, On the Federal Security Service, and On the Countering of Extremist Activities; the Criminal Code of the Russian Federation; the Criminal Procedure Code of the Russian Federation; the Code on Administrative Violations of the Russian Federation; the Civil Code of the Russian Federation; the Federal Constitutional Law on Military Status; and generally recognized principles and norms of international law and ratified international agreements on the fight against terrorism.

These laws determine the legal and organizational foundations for the struggle against terrorism and extremism in the Russian Federation, procedures for the coordination of efforts to combat these phenomena on the part of federal executive-branch agencies, executive-branch agencies of Russian Federation members, public associations, organizations (regardless of their form of ownership), officials, and individual citizens. The laws also set forth the rights, respon-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

sibilities, and guarantees of citizens in connection with the struggle against crimes of a terrorist nature and manifestations of extremism.

A bill entitled On Countering Terrorism is under consideration in the State Duma of the Federal Assembly of the Russian Federation. The provisions of this bill call for clarifying basic concepts regarding the struggle against terrorism, changing the direction of state antiterrorism policy by adopting measures to prevent and suppress terrorist manifestations, and expanding and strengthening the powers of government agencies involved in fighting terrorism. Passage of this bill will make it possible to optimize the legal base for combating terrorism in Russia.

In addition, internal affairs agencies and the internal troops of the Russian Ministry of Internal Affairs are currently guided by the provisions of more than 10 international regulatory and legal acts under the auspices of the United Nations (UN), the Council of Europe, and the Shanghai Cooperation Organization, which define the basic objectives and procedures for the interaction of competent agencies of the various states with regard to preventing, detecting, and suppressing crimes of a terrorist nature.

On August 7, 2000, the Russian Federation ratified the European Convention on the Suppression of Terrorism, and on February 13, 2001, it ratified the International Convention for the Suppression of Terrorist Bombing. Furthermore, on December 14, 2000, the Russian Federation joined 120 states and on April 26, 2004, ratified the UN Convention Against Transnational Organized Crime, committing itself to seek out, prosecute, and expedite individuals suspected of involvement in international organized crime. On July 10, 2002, Russia ratified the International Convention for the Suppression of the Financing of Terrorism and on January 10, 2003, ratified the Shanghai Convention on Combating Terrorism, Separatism, and Extremism.

The interactions of federal executive-branch agencies on matters regarding the struggle against terrorism are regulated by more than 30 regulatory and legal acts intended to provide details on the provisions of laws and acts of the president and the government of the Russian Federation.

Meanwhile, the antiterrorist legal base is in need of certain changes, as well as the development of an entire range of regulations aimed at

- developing the bases of the state management system in the area of preventing and eliminating crisis situations caused by the threat or commission of terrorist acts
- shaping a unified conceptual framework in antiterrorist legislation
- defining the scope of the authorities of entities involved in the struggle against terrorism
- eliminating the sources that support terrorist activities with financial resources
- countering propaganda and ideological support for terrorist activities

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- defining the conditions and procedures for decision making regarding the conduct of counterterrorist operations and the timelines for such operations
- harmonizing at the international level procedures for the extradition of individuals suspected of committing crimes of a terrorist nature

The development and improvement of the regulatory and legal base regarding the secure operation of dangerous facilities and the safe use of dangerous materials and technologies must reflect questions of their degree of protection against terrorist acts and the prevention of the possibility they may be used for terrorist purposes. Efforts must be accelerated to develop the system of federal standards and rules establishing unified requirements for the physical protection of dangerous facilities and materials.

Efforts to improve Russian antiterrorist legislation must take the necessary account of relevant, diverse, and very valuable experience of foreign states and international legislation in this area. This experience must be thoroughly and comprehensively studied on a constant basis, with the involvement of Russian legal experts, officials, and field personnel from the law enforcement agencies, special services, and other ministries and agencies involved with relevant questions of the struggle against terrorism, along with foreign experts, including government officials and independent specialists.

Among the forms of interaction and interagency coordination among entities for countering terrorism are the following:

- organization of board meetings and coordination conferences on problems involved in combating terrorism
- activities under the auspices of joint operational headquarters, working groups, and investigations and operations brigades
- exchange of information, including operations information, on the struggle against terrorism and on sources and channels of drug traffic to counter their illegal circulation and thus cut off sources of financing for terrorist organizations and acts
- maintenance of a unified database on matters concerning the trade in drugs, psychotropic substances, and their precursors and on efforts to counter their illegal circulation (creation of the database was included in Decree 976 of the president of the Russian Federation, dated July 28, 2004, and entitled Questions of the Russian Federal Service for Control of the Drug Trade)
- organization of joint operations to suppress terrorist activities
- joint study and exchanges of personnel from specialized units related to the struggle against terrorism
- joint planning and monitoring of relevant activities

The main goal of this interaction is the formation of a complex and stably functioning interagency system for ensuring the comprehensive protection of all

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

institutions of state power, establishments, enterprises, and citizens against terrorist infringements, thus ensuring that these entities and individuals are fully able to realize their functions, rights, and responsibilities.

The achievement of maximally effective and guaranteed success in antiterrorist activities is largely determined by the clear-cut definition of the functions of the entities involved in it. Based on this premise, the Federal Antiterrorist Commission, as the basic coordinating agency in the fight against terrorism, has been assigned the responsibility of determining the bounds of the responsibilities of each of the participating agencies and cooperative activities, and if necessary, making timely corrections based on an analysis of the current status of the struggle against terrorism and basic trends in the development of this illegal activity. The correctness of the established scopes of responsibility must be carried out at least once every six months, and this review is performed on the basis of requirements of the current operational situation. The main goal of this part of the work of the Federal Antiterrorist Commission is to regulate the work of the interagency system by precluding any duplication in the functions of its component members and ensuring maximal effectiveness of antiterrorist measures by making timely and correct redeployments of the various forces operating in a professional and error-free manner within their assigned spheres.

The distribution of functions of entities for countering terrorism as established by the Federal Antiterrorist Commission defines the scope of the personal responsibilities of officials in exercising their authorities in this sphere. In order to improve the effectiveness of actions aimed at combating terrorism and strengthening the responsibility of officials, the commission at least once every six months organizes and conducts under its auspices a working meeting at which the results of antiterrorist activities are analyzed. The results of these working meetings are incorporated into interagency regulatory documents, which are amended and augmented with practical recommendations developed on the basis of an analysis of weak points in the work of the interagency system and on positive experience accumulated in the most recent period.

To improve the level of interaction among federal executive branch agencies, regional internal affairs departments, and other law enforcement organs with an interest in antiterrorist activities, the following actions would be useful:

- continuing to exchange information with other law enforcement agencies on planned and committed terrorist acts and other illegal interference in the operations of industrial facilities, transport, elements of the information infrastructure, regional internal affairs agencies, and other law enforcements bodies
- establishing the operational exchange of information with the Russian Federal Security Service on persons involved in or suspected of organizing attacks on transportation in the Russian Federation so that such persons may be listed in a timely manner on watch lists for the movement of various types of

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

transport, relevant personnel may be notified, and the secret service apparatus alerted to the need for their detection and processing

- improving the level of interaction with elements of the Russian Ministry of Internal Affairs and its regional subunits in the exchange of information on lost and stolen blank passports with the aim of detecting persons participating in armed formations and committing terrorist acts and halting their illegal presence within the Russian Federation
- regularly holding conferences, seminars, practical exercises, and training courses on the coordination of joint actions by internal affairs agency personnel on transport, at industrial and energy-sector facilities, and in places where large numbers of people gather in order to prevent, detect, and investigate acts of sabotage and terrorism
- creating an information system common to the Russian Federal Security Service and other federal executive-branch agencies that would consolidate information on individuals and legal entities on which there is information regarding possible involvement in the financing of terrorist or extremist organizations, as well as those organizations in which the founders, leaders, and personnel are originally from the North Caucasus region or Central Asia
- continuing efforts to detect and suppress channels by which large sums of cash are moved on various means of transport, including with the involvement of transport system personnel; conducting operational inspections in cooperation with the Russian Federal Security Service of commercial structures and organizations having financial and contractual relations with firms in regions that are unstable from a crime standpoint, including those organizations involved in shipping cargo to such regions

Security agencies interact with

- organizations that manage dangerous facilities and systems for the state accounting and control of dangerous substances, in the course of state monitoring of these facilities and systems
- the Russian Ministry of Internal Affairs, in carrying out inspections of the physical protection of dangerous facilities
- the Federal Security Service, in detecting and investigating cases of illegal access to dangerous materials

The organization of interagency efforts is aimed at ensuring the effectiveness of activities and interagency cooperation among structural subunits of the antiterrorist entities in detecting terrorist and extremist groups, organizations, and societies and preventing them from committing crimes of a terrorist nature or extremist intent, as well as identifying and eliminating the causes and conditions promoting terrorist and extremist activities.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

The organization of interactions among the subunits and regional branches of antiterrorist agencies in their conduct of joint operational-preventive operations and operational-search measures should be determined by departmental regulatory and legal acts, which should include as a top priority the task of uncovering terrorist activities.

As part of the struggle against terrorism and within the bounds of their established competencies, subunits of the various entities involved in antiterrorist activities take part in intra-agency collaboration at all levels in the following main ways:

- planning and conducting, jointly and independently, comprehensive operational-preventive measures and special operations to detect terrorist and extremist groups, organizations, and societies and prevent them from committing crimes of a terrorist nature or extremist aim, as well as detect and eliminate the causes and conditions that promote terrorist and extremist activities
- engaging in a mutual informational exchange of data of interest to the entities involved in antiterrorist activities and directly associated with their performance of tasks and functions assigned to them by legislative and other regulatory legal acts of the Russian Federation
- organizing efforts to monitor the activities of entities involved in antiterrorist activities regarding their compliance with Russian Federation legislation and departmental regulatory legal acts concerning the prevention of crimes of a terrorist nature or extremist aim
- conducting joint hearings on the results of official operational activities
- working in cooperation with interested structural subunits of the entities involved in antiterrorist activities to study, summarize, and disseminate the latest experience of internal affairs agencies and their structural subunits to prevent crimes of a terrorist nature and extremist aim
- exchanging experience with the aim of improving the qualifications of personnel, including by holding joint seminars and conferences and working with research subunits to provide organizational-methodological support for the activities of entities involved in antiterrorist efforts to prevent crimes of a terrorist nature or extremist aim
- participating in inspections and other checkups
- rendering practical assistance to the subunits of entities involved in antiterrorist activities in conducting the most complex operational-search measures to prevent crimes of a terrorist nature or extremist aim
- carrying out joint research on problems associated with antiterrorist and antiextremist activities

In the interest of improving interagency cooperation, the following should be developed, implemented, and improved:

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- plans at the federal and regional level for providing antiterrorist security for facilities that present an increased level of danger (transport, nuclear power, facilities with a heightened level of environmental danger)
- interagency plans for cooperation on particular problems involved with antiterrorist security
- multioption plans for conducting antiterrorist measures and operations when possible changes occur in the operational situation or the algorithm of actions of terrorist structures
- typological options for making management decisions on the use of forces and resources of antiterrorist entities in the struggle against terrorism in particular situations

In fulfillment of Point 6, Article 6, of the Federal Law on the Struggle Against Terrorism, Resolution No. 880 of the Government of the Russian Federation, dated December 10, 2002, established the Federal Antiterrorist Commission. The commission's main task is to develop the foundations for state policy regarding the struggle against terrorism and recommendations for improving the effectiveness of efforts to uncover and eliminate the causes and conditions promoting the rise of terrorism. The commission is also charged with coordinating the activities of federal executive-branch agencies waging the fight against terrorism.

In organizing activities at the federal level within the framework of the Federal Antiterrorist Commission, executive-branch agencies do the following:

- ensure the timely preparation of decisions by the president of the Russian Federation and the government of the Russian Federation on the most pressing problems in this sphere in cooperation with other interested entities involved in the struggle against terrorism
- make proposals and recommendations on development of the foundations for state policy and the improvement of federal legislation on combating terrorism in the Russian Federation aimed at improving the effectiveness of efforts to uncover and eliminate causes and conditions promoting the rise of terrorism and the conduct of terrorist activities
- ensure maximal use of the capabilities of federal executive-branch agencies involved within the scope of their competencies in uncovering, preventing, and suppressing terrorist activities
- present informational and analytical materials on the status and development trends of terrorism in the Russian Federation and facilitate the formation of a unified approach by federal executive-branch agencies (within the scope of their competencies) to objectives involved in the struggle against terrorism
- make recommendations on improving the coordination of activities of federal executive-branch agencies and executive-branch agencies of members of the Russian Federation in order to harmonize their activities to uncover, prevent,

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

and suppress terrorist acts and to uncover and eliminate causes and conditions promoting their preparation and implementation

- participate in the creation and operation of the governmentwide system of measures to combat terrorism

In addition to application of the capabilities of the Federal Antiterrorist Commission, cooperation at the federal level also proceeds within the framework of the activities of regional antiterrorist commissions as well as in the course of contacts with local government agencies, public associations, and organizations involved in the struggle against terrorism within the scope of their competencies.

Nevertheless, given the counterterrorism situation that has taken shape in the Russian Federation, improvements are needed in the organization of cooperation among federal executive-branch agencies in this sphere. The effectiveness of the struggle against terrorism does not depend on the number of power structures created to combat it nor the level to which they report. It is essential to clarify the structure, composition, and functional responsibilities of existing power ministries and agencies and all services involved in the antiterrorist struggle relative to the current situation. To improve the effectiveness of their activities, their operations must be made systemic and coordinated, with controls and strict accountability to be established for officials responsible for carrying out assigned tasks.

Given that terrorism has taken on a nationwide scale in Russia and closely collaborates with international terrorism, the organization, management, and coordination of the activities of the power ministries and agencies is the prerogative of the president of the Russian Federation, who carries out these duties through the Security Council of the Russian Federation.

Development of proposals on implementing the strategy of combating terrorism is the systemic and regular work of interagency commissions and the staff of the Security Council of the Russian Federation and involves the best intellectual and scientific forces in the country.

If a single agency were to be formed to organize, be responsible for, and coordinate the work of all special services involved in the struggle against terrorism, it could be the primary executive-branch agency ensuring the practical implementation of decisions regarding the fight against terrorist manifestations throughout the Russian Federation. The agency's competency must include intelligence and counterintelligence, the fight against terrorism and drug trafficking, the border control service, the governmental communications service, special subunits and security units of the government and important facilities, and scientific-technical subunits.

In addition, the functions of a number of federal ministries and executive-branch agencies of members of the Russian Federation must be clarified and adapted to conditions in antiterrorist activities. The government must make it a

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

top priority to carry out the full technical re-equipment of all law enforcement agencies and to create simplified conditions for the activities of subunits involved in the antiterrorist struggle in their conduct of operational measures.

The main task for cooperation at the federal level is to create conditions that preclude the possibility of criminal actions being committed by terrorist groups and bandit formations on Russian territory, with the aim of completely halting their illegal activities and eliminating opportunities for their appearance. Accomplishing this task will ensure that terrorist activities will be consistently and unshakably curtailed in the Russian Federation.

Efforts aimed at preventing terrorist activities are based on a set of intelligence measures to uncover terrorist groups and bandit formations. These efforts include the following federal structures:

- the Federal Security Service of the Russian Federation, which tracks contacts between terrorist groups and bandit formations and representatives of foreign special services and organizations in the Russian Federation and handles overall coordination efforts on these matters
- the Foreign Intelligence Service of the Russian Federation, which works to uncover possible support for terrorist groups and bandit formations on the part of official and private structures of foreign states
- the Main Intelligence Administration of the Ministry of Defense of the Russian Federation, which is involved in uncovering channels of cooperation between terrorist groups and bandit formation and the military agencies of foreign states
- the Ministry of Internal Affairs of the Russian Federation, which identifies participants in terrorist groups and bandit formations, their places of deployment, and their sympathizers

The coordinating role at this level of antiterrorist activity is assigned to the Federal Antiterrorist Commission of the Russian Federation. While implementing the entire range of antiterrorist measures, the Federal Security Service of the Russian Federation also undertakes comprehensive coordination of plans for antiterrorist measures conducted jointly with the Ministry of Internal Affairs, the Federal Protective Service, and the Ministry of Civil Defense Affairs and Emergency Situations and is responsible for providing timely information and developing practical recommendations to these agencies if complications arise in the operational situation. Each of these agencies takes the following measures as such information is received:

- The Ministry of Internal Affairs amends current work plans so as to improve a range of preventive antiterrorist measures and places its territorial and special subunits on heightened operational status if necessary.
- Based on recommendations received, the Federal Protective Service

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

makes improvements in the system of protection and in extreme situations puts an intensified protection regime mechanism into effect.

- The Ministry of Civil Defense Affairs and Emergency Situations increases its monitoring of compliance with the requirements of security measures at facilities that represent potential targets for terrorist attacks.

In the course of taking these measures, the agencies actively exchange information on the results they have achieved and present reports to the Russian Federal Security Service on their fulfillment of requirements regarding recommendations assigned to them for implementation.

With the aim of working out all aspects of cooperation, joint regional training exercises are held each year under the auspices of the Federal Antiterrorist Commission, with the results being reported to a meeting of the commission involving the heads of all entities involved in antiterrorist activities.

Interagency cooperation is often limited to the scope of operational-technical measures or operational-investigations activities carried out in ongoing case investigations. Meanwhile, the comprehensive and coordinated utilization of forces and resources involved in antiterrorist activities is an irreplaceable condition for success in interagency cooperation.

Copyright National Academy of Sciences. All rights reserved.

Safety and Security in Megacities

Lewis M. Branscomb
Harvard University

> . . . unlike biological communities . . . [the city is] a kind of artificial ecosystem dominated by technology, sustained by natural life support systems and motivated by social behavior. It is a socioeconomic natural complex ecosystem.
>
> —Lu Yongxiang, President, Chinese Academy of Sciences[1]

The world population is already concentrated in cities, and this concentration will continue. Populations around the world are migrating to the greatest cities, seeking economic opportunity and security. If the megacities are able to provide safety and security to their citizens, as well as economic opportunity and social services, there may be many benefits. Declining population in rural areas may reduce stress on natural environments. The efficient aggregation of resources and provision of social services may improve the quality of life. Megacities linked through shared experience and mutual support may emerge as a new pattern of social structures internationally, focused on human needs that nation states often address less effectively. However, the very richness of big city resources is itself a source of vulnerability to a broad range of kinds of disasters.

Big cities, with their high-density populations, are exposed to a variety of threats of disaster; they must be organized to prevent and respond to those disasters, large and small. Traditionally these have been either natural disasters (hurricanes, floods, earthquakes, tsunamis, and so forth) or *technogenic*[2] disasters

[1]Quoted in G. Bugliarello. 2003. Large Urban Concentrations: A New Phenomenon. P. 14 in Earth Science in the City: A Reader, G. Heiken, R. Fakundiny, and J. Sutter, eds. Washington, D.C.: American Geophysical Union. See also Lu Yongxiang. 2001. Eco-Integration: A New Approach in Dealing with the Challenge of Cities' Expansion in Developing Countries. Beijing: Chinese Academy of Sciences.

[2]I am grateful to the Russian delegates to the National Academies-Russian Academy of Sciences conference for this facile adjective to describe system failures resulting from either poor technical design, poor management, or human error.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

resulting from human error and infrastructure that fails to be sufficiently robust. Russia[3] and Japan[4] have taken the view that the newest and most threatening form of disaster—terrorism—should be considered as an extension of the threats for which cities are historically organized. This is the right way to analyze the problem, that is, looking more broadly at safety and security, including terrorism, for two reasons: (1) The agencies and officials who are responsible for dealing with earthquakes, fires, power blackouts, and riots must, in most cases, use the same facilities and capabilities for coping with terrorism, and (2) only this approach allows an affordable and sustainable effort.

Megacities[5] differ from smaller cities not only in their enormous size and high growth rates but also in both the depth and the range of their resources and the complexity of assuring the reliable functioning of all the services on which the city's life depends. Megacities do enjoy concentrations of valuable human and physical resources, but while natural disaster response capability is extensive in many megacities, it is often not sufficient to prevent wide-scale destruction and loss of life. In some megacities neither resources nor political will are sufficient to make megacities significantly less vulnerable. Transportation facilities, for example, may not be adequate to provide for emergency evacuation when necessary. As cities have grown faster than municipal governments can build and adapt their infrastructure to cope with disasters, capabilities such as public transportation have failed to keep up with emergency requirements.

Now one must add to natural and technogenic disasters the threat of social violence, of which the most extreme form is catastrophic terrorism. Social unrest, and its extreme form, terrorism, are very old threats to established societies. In the wake of the end of the cold war, new forms of conflict have proliferated, stimulated by ethnic rivalries, political insurgencies, and religious bigotry, often with deep historic roots. From 1989 to 1999 major incidents of social violence took place in 34 major cities around the world, including some 15 in the Middle East and Asia. The character of the resulting conflicts has changed, however, with civilians as both the targets and the instruments of terrorism, and with new technologies (including the so-called weapons of mass destruction) dramatically expanding the potential for death and destruction.

---

[3]International Science and Technology Center, Moscow City Government, Ministry of Civil Defense Affairs and Emergency Situations of Moscow City. 2003. Safety of Mega-cities: Problems, Solutions, International Experience, Proceedings of an International Conference in Moscow, October 7–9. In English.

[4]USA-Japan Bilateral Conference on Safety and Security. 2004. Tokyo, February.

[5]The United Nations (UN) defines a *megacity* as a metropolitan area of more than 10 million inhabitants. The definition is quite arbitrary, and is also ambiguous, since one may draw the boundary of a metropolitan area arbitrarily.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

MODELS OF MEGACITIES—CRITICAL INFRASTRUCTURES

The interdependent services provided by critical infrastructure make it possible for millions of people to live close together. To the extent the city can protect, control, and manage energy, water, communications, medical, transportation, and emergency services, and can manage the city's resources of food, heavy equipment, and specialized technical skills, a city has many of the tools for responding to and recovering from a disaster of whatever cause.

On the other hand, all of these services, referred to as *critical infrastructure,* are both vulnerable and interdependent. Thus the social impact of an earthquake that knocks out electric power, blocks streets and rail lines, interrupts telecommunications, and ruptures the major conduits for gas and water, is not basically different from a terrorist attack on power stations, transportation facilities, water, and other infrastructure. The major difference between a natural disaster and an intentional terror attack is that the latter can be designed to target specific weaknesses in critical infrastructure and in emergency information and control organizations, and thus have a maximum disruptive effect on a city.

Attacks are likely to involve multiple complex systems. There are a number of dimensions to the systems engineering challenge of homeland security. The multiple critical industrial infrastructures are closely coupled. Almost all of the responses to terrorist threats require the concerned action of federal agencies, state and local authorities, private companies, and in some cases friendly nations. The technologies used in counterterrorism will themselves be coupled complex systems. An evident example is the notion of complex networks of sensors that are coupled to databases, within which the network output is fused with other information and from which sensible information must be provided that local officials in emergency operations centers (EOCs) can use. Thus, priority setting requires modeling and simulating attack and response, red teaming to test the effectiveness of proposed solutions.

Most nations with large cities fail to give adequate attention to the interdependence of the critical infrastructure services on which the city depends. In addition, governments have generally failed to address the realities of human behavior in response to severe disruption of those services and the panic, sickness, injury, and death that may occur on a large scale if more than one of the critical infrastructures fail. The consequences of disasters in megacities fall into six categories. Whether the result of natural, technogenic events, or deliberate attack by terrorists, disasters may be organized into these categories:

1. sickness and death from disease, including illness from contaminated food
2. loss of communications and information services, resulting in weakened decision making and command and control and perhaps panic among the people
3. loss of electric power and fuel supply, affecting all other elements of infrastructure that are not equipped with emergency power generators

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

4. failed or blocked transportation services (air, sea, and land) slowing evacuation from the city and preventing access to incoming medical aid, food, water, heavy equipment, and other resources

5. destruction or toxic contamination of buildings occupied by large numbers of people (especially modern office buildings with fixed windows and central ventilation)

6. vulnerability of people densely congregated in large numbers (in high-density urban neighborhoods or public facilities) to fire, communicable disease, toxic gases, loss of shelter, and panic from terror weapons such as radiation dispersal devices

Each of these threats represents a catastrophic failure in one or more of the city's critical infrastructures. In natural disasters (such as earthquakes) all of these consequences may ensue simultaneously, and each may exacerbate the others. The appearance of an infectious disease, however, may be slow to exhibit symptoms and spread to other people. If the disease is diagnosed and the infected persons are isolated quickly enough, the consequences may be contained. However, many megacities are so densely populated and have such marginal medical facilities that a pandemic, once out of control, would spread very rapidly. With an electric power failure, all other activities may be severely disturbed, as in the 2003 power blackout for about a third of the population of the United States.[6] However, in each case, the magnitude of the cascading of one failure to create the next depends critically on the design of each element of infrastructure.

UNIQUE VULNERABILITIES TO TERRORIST ATTACK

Cities have certain vulnerabilities that are unique to terror attack. The EOCs in many large U.S. cities are quite vulnerable, not only to a destructive physical attack but also to more indirect cyber- or electromagnetic pulse (EMP)[7] attack on their ability to access data and to communicate. Remedying these vulnerabilities must have high urgency; in many cases the centers will have to be relocated.[8]

Much research is already under way to analyze the structural characteristics of high-rise buildings that may make them much more vulnerable than necessary. Without waiting for this research to result in revised building codes, an

[6]Fifty million people lost power in the August 14, 2003, blackout, which resulted in economic losses estimated at between $700 million and $1 billion. One lesson: The wired telephone system, independently powered, remained functional, while cellular phones were overwhelmed.

[7]Devices the size of a suitcase can disrupt sensitive electronic equipment over an area of a city block or more.

[8]The EOC in New York City was located in the World Trade Center, surely not a good choice.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

expert panel of the U.S. National Academies recommended immediate adoption and extension where appropriate of European standards for fire and blast, which were much improved following World War II. Air intakes for large buildings need to be less accessible and should be equipped with better air filters, perhaps with chemical analysis sufficient to determine that toxic or infectious materials are present.

People are the ultimate targets of terror attacks: creating not only death but also fear and panic. The best protection against panic is a quick and accurate diagnosis of the situation, followed by prompt, appropriate, and effective action and clear, transparent information to the public. Effective disbursement of public information is difficult with dispersed authority and accountability.

THE COMPLEXITY, EFFICIENCY, AND VULNERABILITY OF URBAN INFRASTRUCTURES

Many studies of critical infrastructure in the United States have been made over the years. Each time the list grows. Table 1 illustrates the growth of the list of critical infrastructures in the United States from seven in a Congressional Budget Office study in 1983 to 13 in a 2002 White House strategy document. Examination of studies of critical infrastructure suggests that the economies of large, densely populated urban areas are characterized by a combination of independent enterprises, connected in networks of services on which they depend for their ability to deliver goods and services in a highly competitive way. By comparison, a rural agricultural area might be characterized by a high degree of self-sufficiency, with its own food production, the use of wind power for pumping water from wells, and substantial capability to repair machinery. It might have its own electric generators if far from power lines. The primary infrastructure dependencies would be the residual dependency on fossil fuels to operate trucks, tractors, and other machinery.

A 2002 report[9] of the National Academy of Sciences, National Academy of Engineering, and Institute of Medicine attached a high priority to the establishment, within the new U.S. Department of Homeland Security, of a Homeland Security Institute to provide the systems analysis and decision support services to the senior officials in the department.[10] This kind of institution might be a model for megacities as well, since it takes a holistic view of the city and all its interrelated systems: information, physical facilities, infrastructure services, and human behavior.

As economies improve, the richest cities may have more resources than

[9]NRC Committee on Science and Technology for Countering Terrorism. 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C.: The National Academies Press.

[10]Ibid., Ch. 10, pp. 287–312, 344.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 1 Growth in Lists of Critical Infrastructures

1983 Congressional Budget Office	2002 President's Strategy for Homeland Security
Roads	Agriculture
Transit	Food
Wastewater	Water
Water supply	Public health
Air traffic control	Emergency services
Airports	Government
Municipal water supply	Defense industrial base
	Information and telecommunications
	Energy
	Transportation (people and product)
	Banking and finance
	Chemical industry
	Postal and shipping

towns and villages, but big-city critical infrastructures may become more vulnerable to disasters. The physical facilities in which large numbers of people are concentrated are largely in big cities. So too are many of the industrial facilities whose destruction might inflict both economic damage and human injury if toxic substances were released. The responsibility for protecting critical facilities and infrastructure is distributed among private and government owners, and on the government side, among national, regional, and municipal authorities.

A large source of vulnerability of civil society arises from the very efficiency of a competitive economic system. The competitive drive for commercial efficiency creates linkages and vulnerabilities in the critical infrastructure industries. The mechanisms through which the quest for industrial efficiency may threaten an industry's resilience to catastrophe include

- single-point failures: when replacement costs are high, long delays may result from a failure (example: unique ultra-high-voltage transformers in electric power distribution)
- excessive aggregation of production or service in the quest for scale economies (example: in the United States the concentration of chicken meat processing and distribution is in a handful of large firms; in Europe the new Airbus may carry up to 800 passengers)
- coupling to other critical infrastructure systems to leverage their scale economies (example: dependence of transportation safety on availability of electric power and secure computer networks)
- extensive substitution of automated decision systems based on software and networks vulnerable to penetration from remote locations (example: denial-of-service attacks, now familiar in all countries, may be aimed at command and control capability.)

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Thus a competitive economy creates new vulnerabilities, which only government policy and industrial cooperation can reduce. If industry is to bear the cost of these investments, it must make those investments without any reliable means of evaluating risk, and thus the firm may not feel justified in spending the capital. So who will pay to make infrastructure more secure?

This is a serious question, since in the United States the federal government assumes the private sector will make the most important investments to reduce their vulnerability, while the firms, having no reliable way to estimate the risks they face, are reluctant to risk becoming uncompetitive by being first to make such investments. There are alternatives for federal policy to provide appropriate incentives, including

- compulsion through regulation
- subsidies of the research and development to assist in designing the hardening strategies through public-private research and development partnerships (This still leaves industry with the capital expense for implementing the strategy.)
- voluntary commitments with antitrust exemption (The chemical industry in the United States has an excellent record of voluntary standards for plant safety, which might become a model for protection from terrorism.)
- inducing the reinsurance industry to set a sliding scale of rates for terrorism-loss insurance, reflecting the extent to which client firms have invested in measures to reduce vulnerability to disasters

CENTRALIZATION VERSUS DECENTRALIZATION

As previously noted, the organization of critical infrastructure defenses is made complex by the need for government and private business to collaborate in strategy and response to disasters. In the United States there is an additional element of complexity: the presence in most metropolitan areas of multiple political jurisdictions, often quite independent of one another. A striking and perhaps extreme example of this is the Washington, D.C., metropolitan area. Five million people live in this area, but only 572,000 of them reside in the District of Columbia. The district is a federal enclave that functions as the federal seat of government, is legislatively treated for many purposes as a state, but is in fact a city. Within D.C. are found most of the critical targets for terrorists—the Capitol and White House among them. Responsibility for coordinating disasters resides in the D.C. Emergency Management Agency (DCEMA). Its challenge is that it has direct and sole authority over only one disaster response resource—the D.C. fire department. All other resources are controlled by either federal authority or the two states, Virginia and Maryland, that surround it. Counting the counties and cities imbedded in these states, there are 18 political jurisdictions with which

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

the DCEMA must work. Thus the DCEMA can only coordinate information about vulnerabilities, invite its neighbors to cooperate in training exercises, and seek to coordinate all their activities when a disaster strikes the city. To make matters worse, the DCEMA has a very modest budget and operates out of a modest space in a glass-walled building in the northern part of the city.[11] The people who run this facility appear to have done a remarkably effective job, given these constraints, but lacking line authority over the resources required for emergencies, they preside over a highly decentralized structure for disaster response.

This raises an interesting question: What are the relative merits of centralized versus decentralized structures for responding to disasters in megacities? The contrast between the institutional structure in the Washington metropolitan area and in Tokyo, Japan, is striking.

Tokyo has a powerful city government that operates a very sophisticated EOC. The mayor of Tokyo is a powerful political figure in Japan, and he commands the center. The EOC covers two floors of a very large office building that is one of two city office buildings. It is on the seventh and eighth floors, high enough to walk to but out of reach of ground floor attackers. It is very well equipped and organized. I observed an exercise simulating a Richter 7.3 earthquake in downtown Tokyo at this facility.

Each functional service—fire, transport, telecommunications, police, medical services, and so forth—has its own operations center, with the staff dressed in uniforms of immediately identifiable colors.

Status information is fed up from hundreds of local community officials to a central planning room. A much larger command center, on the scale of a manned space launch control room, brings the mayor, his top advisors, and heads of all the functional services together for strategic decisions. On a full-time basis the mayor is represented by retired Lt. General Toshiyuki Shitaka, who brings a high level of discipline to the complex operations of the center.

Central control, as evidenced in Tokyo, has great effectiveness advantages. Through subordinates the mayor of Tokyo has line authority over the component resources, and he can ensure a general budget for the EOC and its staff. The center is equipped with very modern and capable information technology (IT) equipment. For natural and technogenic disasters, the Tokyo center is adequately protected. However, it is not invulnerable, and for certain classes of terrorism attacks with weapons of mass destruction, it might not be adequately protected.

The DCEMA, on the other hand, has very limited authority and limited resources. It is also evidently vulnerable to any attack that would break the glass covering one side of the control room. If, however, the DCEMA were to be

[11]Three and half years after the September 11, 2001, attack, ground has been broken for a new facility for the DCEMA, designed as an operations control center for disasters in the D.C. metropolitan area. The DCEMA also has two mobile facilities and two remote facilities with much, but not all, of the communications capability of the main EOC.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

made ineffective, there are multiple layers of services, including federal military and D.C., Virginia, and Maryland National Guard forces, that could provide some infrastructure to knit together all the separate first responder services in the 18 political jurisdictions that comprise the Washington metropolitan area.

The primary conclusion from this comparison of centralized and decentralized organizations is that the differences may be large when faced with a deliberate attack from terrorists, but the centralized and decentralized facilities are perhaps comparable in capability when responding to natural and technogenic disasters. One of the major advantages of a well-structured, centrally commanded emergency operations authority is the potential to provide uniform, credible information to the public. This would in theory be provided by the DCEMA, but in a major terrorist disaster, political officials such as the president, two governors, and secretaries (ministers) in charge of military and homeland security resources would very likely provide mixed messages.

THREE AREAS FOR POSSIBLE COOPERATION BETWEEN THE U.S. AND RUSSIAN ACADEMIES

Modeling Cities and Their Infrastructure

Unless infrastructure services most critical in a disaster can be modeled and simulated it will be very difficult to assess a city's vulnerability under various disaster scenarios. These models would have to include modeling relationships between government and private institutions, and across interdependent infrastructures and independent government authorities. In addition there is a need to model management of disasters, and especially terror attacks, under both centralized and decentralized command structures. High levels of professional skill at complex systems modeling are required; a sharing of ideas about methods and data could be helpful in both countries.

Need for a Sustainable Strategy

As the frequency of disasters of ever greater consequence declines, the public's attention wanes, as does its tolerance for the costs and inconvenience of measures to reduce vulnerability to improbable but high-consequence events. On the other hand, natural disasters and threats of terrorism will always exist, and a sustainable strategy is necessary.[12]

The goal of disaster avoidance and mitigation should be safety and security, with the understanding that security must include the threat of terrorism. The

[12]Branscomb, L. M. 2004. Protecting civil society from terrorism: the search for a sustainable strategy. Technology in Society 26(2-3):271–285. http://authors.elsevier.com/sd/article/S0160791X04000053.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

public needs to understand that the resources to deal with the most likely disasters pay for most of the risks the city faces. Terrorism is an added cost because it introduces different threat patterns.

The technical strategy must attempt to maximize dual benefits to economy and security through the development of appropriate technologies and procedures. To the extent that costs of vulnerability reduction can be reduced or offset by improved quality of infrastructure services, the public will be more willing to support investments to mitigate very unlikely but high-consequence events.

Collaborative Learning Between Megacities

As cities work to become both safer and more secure, there are opportunities for international collaborative learning between megacities. Because the analytical work is so complex, a pair of major cities such as Moscow and Los Angeles might find that engaging the two academies of sciences as partners in such collaboration to be mutually beneficial.

Copyright National Academy of Sciences. All rights reserved.

The Role of Science and Technology in Homeland Security and Countering Terrorism: Overview of Key Activities at the National Academies[1]

Wm. A. Wulf
National Academy of Engineering

PREFACE

This document provides an overview of National Academies' activities that are relevant to various aspects of homeland security and countering terrorism, particularly catastrophic acts of terrorism. A longer report summarizes a number of individual reports; here we only list their titles.

While much of the National Academies' work—as well as interest in that work—has occurred since September 11, 2001, this paper includes relevant studies and other activities many years before that infamous date. This summary also identifies activities other than studies resulting in academy reports, such as workshops, roundtables, and colloquia that have been and are currently being carried out across the National Academies in this area. Finally, a number of activities in the advanced planning stages are identified.

Many of these activities were spawned directly or indirectly by the delivery of the June 2002 National Academies report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*.[2]

This summary is not exhaustive, especially as to planning efforts. However, it is extensive, including many of the past, present, and planned efforts across the National Academies in these important areas.

---

[1]Activities as of May 2004.

[2]NRC Committee on Science and Technology for Countering Terrorism. 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

INTRODUCTION

The horrific events of September 11, 2001, overshadowed much in all of our lives for many months following. Many in the science and technology community have held that while advanced technology often is used as an instrument of terrorism, technological tools can also be a vital source of prevention and deterrence of, and defense against, acts and agents of terrorism.

The National Academies responded to the terrorist attacks of September 11, 2001, in several ways. First, the presidents of the National Academies at the time, including National Academy of Sciences (NAS) President Bruce Alberts,[3] National Academy of Engineering (NAE) President Wm. A.Wulf, and Institute of Medicine (IOM) President Kenneth Shine,[4] convened a meeting of leaders from the science, technology, and health care communities with leading former government officials to consider initiatives that might be carried out by the National Academies that would benefit the nation. This meeting, the Presidents' Meeting on Countering Terrorism, was convened on September 26, 2001, just two weeks after the terrorist attacks.

A number of key activities resulted from the presidents' meeting, the most prominent of which was the initiation of a major National Academies' fast-track study, A Science and Technology Agenda for Countering Terrorism, aimed at defining very quickly (within six months) a research agenda for enhancing the role of science and technology in countering terrorism in the United States. That study resulted in the previously mentioned landmark report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. That report was used prominently in developing the legislation establishing the mission, structure, and other features of the Science and Technology Directorate in what was to become the U.S. cabinet-level Department of Homeland Security (DHS). As the U.S. government began to implement various measures for homeland security, the implications for the scientific and engineering community became clearer, and in October 2002 the presidents of the National Academies issued a statement on behalf of the National Academies, "Science and Security in an Age of Terrorism."[5]

In addition, as federal agencies began reorganizing activities in waging the war on terrorism, including the 22 agencies that would ultimately comprise DHS, the new focus in government precipitated a variety of other activities across the National Academies. These complemented the significant number of relevant

[3]Bruce Alberts' term as NAS president was from July 1, 1993–June 30, 2005, and he was succeeded by Ralph J. Cicerone on July 1, 2005.

[4]Kenneth Shine's term as IOM president concluded on June 30, 2002, and former Harvard University Provost Harvey Fineberg was appointed the IOM's seventh president, beginning a six-year term on July 1, 2002.

[5]Available on the National Academies Web site: www.nationalacademies.org.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

National Research Council (NRC) projects that predated the events of September 11, 2001, including completed reports and work under way. As a result, there is now a very substantial portfolio of relevant products, projects, and other activities, including the continuing initiation of new work to aid the nation's response to the threat of catastrophic terrorism.

This document summarizes the current portfolio of completed reports, other products, current projects, projects in preparation, and other efforts in support of government agencies and other sponsors.

COMPLETED REPORTS AND OTHER ACTIVITIES

Some of the activities initiated at the National Academies in recent years have been aimed at providing immediate near-term advice to the government, some refocused ongoing efforts to better meet the needs of federal agencies after September 11, 2001, and some were aimed at helping design a long-term agenda for the role of science and technology in countering catastrophic terrorism. The list is long and growing.

A Science and Technology Agenda for Countering Terrorism

This keystone project, noted earlier, initiated in the weeks following September 11, 2001, was aimed at helping the federal government, and more specifically the Executive Office of the President through the Office of Science and Technology Policy and Office of Homeland Security, to use effectively the nation's and the world's scientific and technical community in a timely response to the threat of catastrophic terrorism. A committee of distinguished scientists and engineers, supported by similarly distinguished panels, developed an integrated science and technology program plan and research strategy.

In all, 164 distinguished and knowledgeable individuals, comprising 24 committee members, 94 members of the supporting panels, and 46 expert reviewers, contributed to the effort, which was sponsored entirely by internal resources from the National Academies. The final report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, was released in June 2002. The report provides a framework for the application of science and technology for combating terrorism and proposes research agendas in nine key domains: biological; chemical; nuclear and radiological; information technology; transportation; energy facilities, cities, and fixed infrastructure; behavioral, social, and institutional issues; robotics; and systems analysis and engineering.

Through its influence on the programs and planning within government agencies that have responsibilities for homeland security and countering terrorism, this report has provided the context for many of the follow-on efforts described in this document.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Near-term Assistance to the U.S. Government

To provide timely assistance on those urgent topics where the government needs immediate assistance, the National Academies initiated a new kind of activity. The National Academies' management and staff called upon and continue to call upon a formidable network of scientific, engineering, and health expertise to arrange one-day meetings between scientific experts and government representatives in areas where urgent knowledge was being sought by government agencies. Although no written reports have been produced and no formal advice is provided, the dialogue has proved to be very beneficial to federal agencies, especially the interagency Technical Support Working Group (TSWG) on counterterrorism, the intelligence community, the U.S. Government Accountability Office (GAO), the Federal Aviation Administration (FAA), the Postal Service, and the Department of Justice (DOJ).

The meetings arranged to date in the areas of homeland security and countering terrorism include the following agencies and topics:

- Postal Service on sanitizing the mail (November 14, 2001)
- FAA on analyzing human factors for the FAA's sky marshal program (December 5–6, 2001)
- DOJ on analyzing the anthrax-infected letter to Senator Leahy (December 7, 2001)
- TSWG on surveying the state of the art on biological and chemical forensics (December 11, 2001)
- TSWG on surveying the state of the art on biological and chemical decontamination (December 14, 2001)
- TSWG on through-structure imaging and explosives detection (March 26, 2002)
- GAO on biometric identification (April 25–26, 2002) and on privacy concerns and policy implications of new biometric technologies (May 16–17, 2002)
- Federal Bureau of Investigation on high-performance computing (September 4–5, 2002)
- GAO on assessment of cybersecurity technologies for critical infrastructure protection (October 1–2, 2003)
- GAO on assessment of DHS/Transportation Security Administration (TSA) transportation security research and development (March 2, 2004)
- GAO on security efforts for federal real property (March 4–5, 2004)

Some of these efforts have led to more extensive National Academies projects.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Reports Available from the National Academies Press

In response to requests by government agencies, the National Research Council and the Institute of Medicine have initiated new activities and called upon a substantial body of work already completed. Many of these requests and responses are designed to result in traditional NRC or IOM committee reports. The following compilation is a collection of reports and other documents relevant to the subjects of homeland security and countering terrorism that are available from the National Academies Press.[6] The documents are grouped in general chronological order, but substantively span the following five principal areas, although many of these reports (and other activities) cover more than one topic area. The principal areas covered are the following:

1. critical infrastructure protection
2. detection and mitigation of catastrophic terrorist threats, including radiological and nuclear, chemical, biological, and explosives
3. border and transportation security
4. information analysis, management, and infrastructure protection
5. threat and vulnerability, testing, and assessment, including addressing the root causes of terrorism, coping with new risks, emergency preparedness and response, and international issues

Reports Published in 2004

Forensic Analysis: Weighing Bullet Lead Evidence
Distribution and Administration of Potassium Iodide in the Event of a Nuclear Incident
Advanced Energetic Materials
Improving the Characterization Program for Contact-Handled Transuranic Waste Bound for the Waste Isolation Pilot Plant
Biotechnology Research in an Age of Terrorism
University Research Centers of Excellence for Homeland Security: Summary Report of a Workshop
The Mathematical Sciences' Role in Homeland Security: Proceedings of a Workshop
Advancing Prion Science: Guidance for the National Prion Research Program
Summary of the Power Systems Workshop on Nanotechnology for the Intelligence Community: October 9-10, 2003, Washington, D.C.

[6]Either in printed form from the National Academies Press or the Joseph Henry Press, or available on the National Academies Press Web site at http://www.nap.edu. The Terrorism and Security Collection may be viewed at http://www.nap.edu/collections/terror/index/html.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Overcoming Impediments to U.S.-Russian Cooperation on Nuclear Nonproliferation: Report of a Joint Workshop
Terrorism—Reducing Vulnerabilities and Improving Responses: Proceedings of a U.S.-Russian Workshop

Reports Published in 2003

Review of EPA Homeland Security Efforts: Safe Buildings Program Research Implementation Plan
A Review of the EPA Water Security Research and Technical Support Action Plan: Parts I and II
Assuring the Safety of the Pentagon Mail: Letter Report
Preparing for the Psychological Consequences of Terrorism: A Public Health Strategy
Cybersecurity of Freight Information Systems: A Scoping Study—Special Report 274
Who Goes There? Authentication Through the Lens of Privacy
An Assessment of Non-Lethal Weapons Science and Technology
Science and Technology for Army Homeland Security: Report I
ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects: A Review and Commentary
Tracking and Predicting the Atmospheric Dispersion of Hazardous Material Releases: Implications for Homeland Security
Critical Information Infrastructure Protection and the Law: An Overview of Key Issues
The Internet Under Crisis Conditions: Learning from September 11
Information Technology for Counterterrorism: Immediate Actions and Future Possibilities
National Security and Homeland Defense: Challenges for the Chemical Sciences in the 21st Century
Microbial Threats to Health: Emergence, Detection, and Response
Accelerating the Research, Development, and Acquisition of Medical Countermeasures Against Biological Warfare Agents: Interim Report
Advancing Prion Science: Guidance for the National Prion Research Program—Interim Report

Reports Published in 2002

Countering Agricultural Bioterrorism
Cybersecurity Today and Tomorrow: Pay Now or Pay Later
IDs—Not That Easy: Questions About Nationwide Identity Systems
Countering Terrorism: Lessons Learned from Natural and Technological Disasters

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Biological Threats and Terrorism: Assessing the Science and Response Capabilities: Workshop Summary
Protecting Our Forces: Improving Vaccine Acquisition and Availability in the U.S. Military
The Anthrax Vaccine: Is It Safe? Does It Work?
Countering Bioterrorism: The Role of Science and Technology
An Assessment of the CDC Anthrax Vaccine Safety and Efficacy Research Program
Summary—Assessment of Technologies Deployed to Improve Aviation Security: Second Report: Progress Toward Objectives
Preparing for Terrorism: Tools for Evaluating the Metropolitan Medical Response System Program
Discouraging Terrorism: Some Implications of 9/11
High-Impact Terrorism: Proceedings of a Russian-American Workshop
Summary—Assessment of the Practicality of Pulsed Fast Neutron Analysis for Aviation Security
2001-2002 Assessment of the Army Research Laboratory[7]
Letter Report of the Committee on Assessment of Technologies Deployed to Improve Aviation

Reports Published in 2000 and 2001

Protecting People and Buildings from Terrorism: Technology Transfer for Blast-effects Mitigation
Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism
Summary of Discussions at a Planning Meeting on Cyber-Security and the Insider Threat to Classified Information
Blast Mitigation for Structures: 1999 Status Report on the DTRA/TSWG Program

Reports Published Before 2000

Improving Surface Transportation Security: A Research and Development Strategy, 1999
Fire- and Smoke-Resistant Interior Materials for Commercial Transport Aircraft, 1995
Improved Fire- and Smoke-Resistant Materials for Commercial Aircraft Interiors: A Proceedings, 1995

[7]This report is not available on the National Academies Press Web site, and may be accessed by contacting the Public Access Records Office of the National Academies at 202-334-3543.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

New Materials for Next-Generation Commercial Transports, 1996
Protecting Buildings from Bomb Damage: Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications, 1995
Use of Underground Facilities to Protect Critical Infrastructures: Summary of a Workshop, 1998
Airline Passenger Security Screening: New Technologies and Implementation Issues, 1996
Black and Smokeless Powders: Technologies for Finding Bombs and the Bomb Makers, 1998
Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response, 1999
Configuration Management and Performance Verification of Explosives-Detection Systems, 1998
Containing the Threat from Illegal Bombings: An Integrated National Strategy for Marking, Tagging, Rendering Inert, and Licensing Explosives and Their Precursors, 1998
Detection of Explosives for Commercial Aviation Security, 1993
The Practicality of Pulsed Fast Neutron Transmission Spectroscopy for Aviation Security, 1999
Balancing Scientific Openness and National Security Controls at the Nuclear Weapons Laboratories, 1999
Computers at Risk: Safe Computing in the Information Age, 1991
Computing and Communications in the Extreme: Research for Crisis Management and Other Applications, 1996
Cryptography's Role in Securing the Information Society, 1996
Realizing the Potential of C4I: Fundamental Challenges, 1999
Summary of a Workshop on Information Technology Research for Crisis Management, 1999
Trust in Cyberspace, 1999
Assessment of Future Scientific Needs for Live Variola Virus, 1999
Assessment of Technologies Deployed to Improve Aviation Security: First Report, 1999
Aviation Fuels with Improved Fire Safety: A Proceedings, 1997
Fluid Resuscitation: State of the Science for Treating Combat Casualties and Civilian Injuries, 1999
Improving Civilian Medical Response to Chemical or Biological Terrorist Incidents: Interim Report on Current Capabilities, 1998
Proliferation Concerns: Assessing U.S. Efforts to Help Contain Nuclear and Other Dangerous Materials and Technologies in the Former Soviet Union, 1997
Protecting Nuclear Weapons Material in Russia, 1999
The Protection of Federal Office Buildings Against Terrorism, 1988

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Other Projects

Safety of the Nation's Water Supplies
Forum on How Natural Disaster Research Can Inform the Response to Terrorism
Interdependent Vulnerabilities for Critical Infrastructure Protection
Balancing National Security and Open Scientific Communication: Implications of September 11 for the Research University
General Education of the Media and Public on Terrorism Vulnerabilities and Responses
Forum on Microbial Threats
IOM Council Statement on Vaccine Development
Scientific Openness and National Security

Additional International Projects

International Workshop on Implications of Trends in Chemical Science and Technology for Chemical Weapons and Chemical Terrorism
Facilitating International Scientific Meetings in the United States
Monitoring Foreign Students
U.S. Government Efforts/Needs to Restrict Dissemination of Data in Light of New National Security Concerns

ONGOING NATIONAL ACADEMIES ACTIVITIES

A wide range of traditional NRC/IOM studies and other activities are under way in the general area of counterterrorism. The following summarizes many of those activities.

Active Committees and Reports in Preparation

Army Science and Technology for Homeland Defense: C4ISR-Phase II
An Assessment of Naval Forces' Defense Capabilities Against Chemical and Biological Warfare Threats
Improving Cybersecurity Research in the United States
U.S. Government Research and Development in Support of Cyberassurance for the Critical Infrastructure of the United States
Nanotechnology for the Intelligence Community
Review of Testing and Evaluation Methodology for Biological Point Detectors
Assessment of Technologies Deployed to Improve Transportation Security
Educational Paradigms for Homeland Security
Safety and Security of Commercial Spent Nuclear Fuel Storage
Establishing Priorities for U.S.-Russian Cooperation in Countering Radiological Terrorism

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Review of Research Proposals for Cooperation with Former Soviet Biological Weapons Personnel and Institutes
Future Contributions of the Biosciences to Public Health, Agriculture, Basic Research, Counterterrorism, and Nonproliferation Activities in Russia
Roundtable on Scientific Communication and National Security
Indo-U.S. Science and Technology Workshop to Counter Terrorism
Protection, Control, and Accounting of Nuclear Materials: International Challenges and National Programs—Workshop Summary
Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats

Other Activities Under Way or in Advanced Planning Stages

In addition to traditional NRC studies and related program initiation activities, many units across the National Academies have initiated other kinds of activities relevant to the general area of countering terrorism. The follow summarizes some of those projects.

- The News Media and First Response
- Transportation Research Board (TRB) Cooperative Research Programs
- National Cooperative Highway Research Program Security Projects

  ◊ Transportation Security
  ◊ A State DOT Field Personnel Security Manual
  ◊ Methods for Determining Transportation and Economic Consequences of Terrorist Attacks
  ◊ Secure Communication Infrastructure
  ◊ Emergency Traffic Operations Management
  ◊ Transportation Response Options: Scenarios of Infectious Disease, Biological Agents, Chemical, Radiological, or Nuclear Exposure
  ◊ Bridge/Tunnel/Highway Infrastructure Vulnerability Assessment Workshops

- Transit Cooperative Research Program Security Projects

  ◊ A Guide to Public Transportation Security Resources
  ◊ Prevention and Mitigation
  ◊ Security-related Training and Customer Communications: Lessons Learned from September 11 by Transportation Providers
  ◊ Intrusion Detection for Public Transportation Facilities
  ◊ Emergency Response Mobilization Strategies and Guidelines for Transit
  ◊ Use of Portable Explosive Detection Devices
  ◊ Robotic Devices

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

◊ Communication of Threats: A Guide
◊ Transit Security Use of Dogs: A Guide

In response to the terrorist attacks of September 11, 2001, TRB initiated a number of new activities and expanded existing activities aimed at providing tools to assist state, local, and national transportation agencies in deterring, preventing, detecting, mitigating, responding to, and recovering from terrorist attacks. These tools include the following:

- TRB Transportation Security Web site
- Transportation Security
- A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents
- A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection
- Methods for Improving Transit Security
- Emergency Preparedness for Transit Terrorism
- Terrorism Prevention and Mitigation for Transit Systems
- Public Transportation Security, Volume 1: Communication of Threats
- Future Tools and Resources
- TRB Program Initiation Activities

PROSPECTIVE ACTIVITIES: NRC/IOM STUDIES AND OTHER WORKSHOPS, MEETINGS, AND PROJECTS IN PLANNING STAGES

Reducing the Physical and Economic Vulnerability of the United States to Threats to the Chemical Supply Chain
Joint Committee on U.S.-Russian Cooperation on Nuclear Nonproliferation
Response to Global Terrorism: Continuation of the U.S.-Russian Interacademy Project on Conflicts in Multiethnic Societies
Science and Technology in U.S. Foreign Assistance Programs—Implications for AID and its Partners
U.S.-Russian Interacademy Project on Counterterrorism
International Forum on Biosecurity
Indo-U.S. Cooperation to Counter Infrastructure Terrorism: Workshop on Threats to Communications Systems and Public Transportation Systems
Emergency Preparedness for Terrorist Events: Emerging Opportunities for Science and Technology
Understanding Terrorism
Examining the Science Base for Microbial Forensics
Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare
Maintaining the Safety and Security of U.S. Water Systems

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Understanding, Coping with, and Combating Terrorism: Potential New Initiatives in DBASSE

CONCLUDING COMMENTS

Defining the role of science and technology in homeland security and countering terrorism has emerged over the past year as a prominent theme of activities across the National Academies. The National Academies portfolio spans the spectrum to varying degrees of the domains of prevention, detection, response, and recovery as well as analyzing key areas of potential terrorist threat, including biological, chemical, nuclear, and radiological threats; cyberterrorism; and vulnerability of the nation's infrastructure, including transportation, energy facilities, cities, and other fixed infrastructure. Finally, the portfolio also includes a number of efforts aimed at a better understanding of the root causes of terrorism.

The heightened sentiments regarding sensitive but not classified features of many of these activities have added a dimension of complexity to the National Academies' approach to dealing with these issues, which had traditionally fallen fairly clearly into classified and unclassified domains with routine procedures for handling information and disseminating reports in either case. This complexity is exacerbated in the context of our public disclosure obligations under Section 15 of the Federal Advisory Committee Act. Many officers and staff are involved in fashioning ways to function in the new environment, while federal policy continues to evolve.

Copyright National Academy of Sciences. All rights reserved.

Does the Emergence of Insurgencies Provide Lessons for Terrorism?

Robert McC. Adams
University of California at San Diego

It is important to note at the outset that the Russian Academy of Sciences-National Academies Project on Conflict and Reconstruction in Multiethnic Societies was initiated in early 2000, preceding the terrorist attacks of September 11, 2001, in the United States. Hence it originally had the substantially broader focus that its title suggests than the general subject of this meeting. The scope of activities as it was then anticipated is largely reflected in the publication of the proceedings of a U.S.-Russian workshop, *Conflict and Reconstruction in Multiethnic Societies*.[1] This concern for relatively diffuse and heterogeneous sources of violence has been somewhat but not completely overtaken by the impacts of rapidly developing international networks of a generally Islamist, more specifically terrorist, character. By design, the binational group was composed of scholars seeking to establish broad patterns with a comparative approach, and not with individuals having the real-time concerns of national policy makers and those charged with the active suppression of terrorist acts.

In fact, this experience leads me to believe that terrorist activity can be better explained by placing it in a fairly wide array of insurgent movements, rather than by focusing on a wholly committed terrorist group. Engagement in degrees of arguably terrorist activity extends across an irregular continuum, from occasional, part-time, and even one-time participation to full-time involvement. By far the larger numbers of those falling to some degree under this heading are

[1]NRC Committee on Conflict and Reconstruction in Multiethnic Societies. 2004. Conflict and Reconstruction in Multiethnic Societies: Proceedings of a Russian-American Workshop. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

in the less committed category, and most of their behavior and ideas blend into those of much larger groups of which they remain members.

Core groups of fully committed terrorists have exhibited serious, sophisticated concern for their own security. The conspicuous lack of success that U.S. and Iraqi national forces have had in capturing members of the al-Zarqawi leadership is evidence of that. On the other hand, emphasis on a tight-knit cellular structure amplifies such groups' prevailing difficulties and slowness in communication with its dispersed members. This has the effect of loosening central control and encouraging independence of action. Moreover, in a context of widespread support for insurgency and publicly perceived terrorist effectiveness against seemingly overpowering military forces, new cells quickly form and take action on their own while typically exhibiting less and less concern for unity of program and action. Again, this is being repeatedly demonstrated not only in Iraq but also in Western Europe. Hence there are multiplying targets for antiterrorist intelligence and action, presenting widely differing degrees of difficulty of access. It cannot be an acceptable strategy for counterterrorist policy makers to narrow their focus to what they, but not necessarily the subject population at large, perceive as the original, innermost circles at the heart of the challenges they face.

More spontaneous and marginal participants have not infrequently proved to be approachable by journalists and unofficial informants. While some insights into the dynamics of these groupings can be gained in this way, as well as from comparative and historical data, specific, time-sensitive, action-oriented, information is prevailingly beyond reach.

Valery Tishkov's early warning networks are a useful innovation that rely on the reporting by trained local observers of depersonalized, essentially contextual criteria to identify impending conditions of threat or tension, but they, too, have limits. Typically extended and intense, fully candid networks of communication tend to shrivel up as tensions rise, so that when we most need them they become progressively more circumscribed and fragile.

Great states that are victimized by terrorism may resist accepting this, but rigid definitions of what is terrorism are elusive and contentious. Targeting civilian noncombatants is a common shorthand description, but it has obvious limitations in situations of asymmetrical warfare. Are there genuine noncombatants when much of a region's population is either actively up-in-arms or at least passively in support of those who are? Insurgents have to make use of the crude, low-tech, not very selective weapons they can readily seize or have at hand. Organized military forces, on the other hand, make use of much more powerful and destructive weapons, particularly air and heavy artillery bombardment, and then too frequently dismiss attendant civilian casualties as mere collateral damage. The affected population, of course, may view this differently. Certain egregious acts clearly qualify as terrorism, and certain organized groups like al Qaeda clearly see themselves as systematically engaged in exploiting precisely such

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

egregious acts to enhance their reputation for fearful conduct. I am personally uneasy when the uniform characterization of terrorist is used without qualification along its wide and heterogeneous borderlands.

Terrorism in varying forms has appeared in other, earlier times and settings. We should not forget the current or recent examples of the Red Brigades, the Irish Republican Army (IRA), the Euskadi Ta Askatasuna (ETA), and the Tamil Tigers, among others. Modern occurrences, most generally, are in contexts that blur the line—certainly in the perceptions of contending participants—between terrorism per se and some other types of insurgent (for example, religious, ethnic, or nationalist) violence. Typically the contexts involve what is locally perceived as longstanding, repressive discrimination in access to land, employment, education, and other resources, or military occupation that forecloses other, less violent types of civic protest or even involvement. This clearly does not provide an acceptable rationale for what committed terrorists are trying to do, but it drastically loosens all existing restraints on the wider communities in which they move. Intersecting networks of large and small grievances are formed, for which no orderly remedies are in sight.

Leaving aside full committed terrorist cadres, individuals living in an insurgency thus often find themselves confronting multiple pressures calling for allegiance with or opposition to other organized groupings in their immediate surroundings. Dominant personal selections among these alternative identifications naturally are at first fluid, unstable, rarely well articulated or perhaps even understood. Peer pressure is obviously a factor in recruitment, but so are older attachments and rivalries, and even events that may range in scale from major to microscopic. Urgently we would like to obtain some general insights about relations between terrorists and the societies that sustain them (not completely unwillingly, or the terrorist cores could not operate and survive).

In trying to find a constructive path through this conundrum there is an approach that deserves serious consideration. What can be learned from manifestations of civic violence involving the emergence of insurgent formations to which the term terrorist applies only questionably or not at all? Here our focus is on better understanding the dynamics of group formation under conditions of widely prevailing violence, if that permits us to learn from examples that are relatively more open to serious investigation. While one cannot take for granted that any such examples are similar in their essentials to the challenges of terrorism confronting us today, they may at least guide us to a better understanding of some important aspects of the problem, for example, on how insurgencies

- recruit their members, and then sustain themselves in the face of withering losses to better armed adversaries
- relate to the relatively more passive population around them from which they themselves are drawn

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- establish and communicate the goals for which they are ready to fight and make sacrifices
- generally have to settle for at best very partial successes

An outstanding example of a study of this kind deserves brief description, emphasizing once again that it is insight into processes of insurgent group formation, coherence, and effective action amid sacrifices we are looking for, not rules that apply with any closeness of fit to the subject of countermeasures to terrorism that brings us together. I refer to a very recent monograph by Elisabeth Wood, *Insurgent Collective Action and Civil War in El Salvador*.[2] On the basis of sensitive, long-continuing fieldwork, she traces evolving forms of militant peasant collective action in a series of representative Salvadoran case-study areas.

Collective violence first occurred there in connection with a mass social movement in the mid-1970s. By the early 1980s a loosely knit insurgent army had come into being, with scattered but vital covert support. Around this there emerged a vibrant civil society, capable of holding its own in what became a military stalemate. Wood conducted extended interviews over many years with hundreds of insurgents, landlords, nonparticipants, and commanders of military and guerilla forces. By repeated, extended, ultimately interlocking cross-checking of individuals' own accounts of their motives and actions with those of other participants, she was able to establish a high, although she is careful to insist never absolute, level of veracity. The prevailing form of collective action was the seizure of lands from great haciendas and its distribution among militant cooperatives.

A very heavy price was paid for this, the result of long-continuing, low-intensity warfare with regular military forces and vigilante death squads, assassinations, and unaccounted-for disappearances. From an annual high of around 20,000 war-related deaths in 1980, it tapered off to 2,000 or so in 1984 and stabilized there until peace was negotiated after 1990. El Salvador today faces other problems in maintaining a course of economic development and dealing with massive emigration, but the insurgent cooperatives have largely secured their place in a new, relatively stable social order. Still, as one rebel activist noted with apparent puzzlement some years later, "We shed blood all these years [just] in order to buy land at market prices?"

Wood was at pains to probe the question of motivation. Personal gain she found she had to exclude: At great personal risk and loss, the insurgents shared what was won completely with nonparticipants. Similarly, she could not identify a pattern of preexisting community loyalty and well-established social networks.

[2]Wood, E. 2003. Insurgent Collective Action and Civil War in El Salvador. New York: Cambridge University Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Two-thirds of the residents in the areas studied lent no active support to the insurgents. Instead, Wood finds that the backgrounds and motivations of the insurgents were highly diverse, from personal grievances and perceived injustices to liberation theology. Her important conclusion is that, once joining the insurgency, individuals all "took pride, indeed pleasure, in the successful assertion of their interests and identity"—in what she terms the "pleasure of agency." In short, insurgents "were motivated in no small part by the value they put on taking part in the making of history."

A unifying set of themes was characteristic of those campesino-insurgents who engaged in and actively supported the insurgency—resentment at the social conditions before the war, aspirations for a different, hopefully more just social and economic order, moral outrage at earlier repression, and pride in what the insurgency achieved. All these themes were muted or absent in interviews with those who did not support the insurgency. This strongly suggests that a new political culture emerged during the civil war among those who supported and joined the insurgency. From diverse beginnings, their political identities were transformed through the struggles of the years of civil war. A new, more explicitly political culture emerged as the insurgent formations constituted themselves and took action, at the same time shaping those involved into new identities as militant activists. "[I]t was participation, rather than other factors," Wood concludes, "that accounts for insurgent political . . . culture."

Insurgency is an emergent phenomenon, in other words. Its shape and dynamic follow no general laws of cause and effect but instead are outcomes of highly complex processes of feedback and interaction. Does the same apply to terrorism as a subset of insurgencies, and in particular to the radical Islamist variety of it that the world now confronts? I am very skeptical of any overall pattern of congruence, as noted earlier, but at the level of a newly emergent organizational structure that generates its own identities and loyalty, this at least deserves serious consideration. Efforts to deal with indigenous practices or occasions of terrorism may need to have the same flexibility of structure, goals, and tactics and a readiness both for sudden, resolute advance and strategic compromise or withdrawal, as was characteristic of other insurgencies like the well-reported one in El Salvador.

In contrast, foreign, internationally moving and communicating networks of fully committed terrorists are an essentially different question. Rootless in a given country of operations, they are relatively unrestrained by gradations and qualifications of support from the population of the host country. Moreover the psychological and socioeconomic impacts they seek are international, with little regard for the interests of the host country. As a result, their growing influence and (perhaps exaggerated reputation for) effectiveness is perhaps the most dynamic and dangerous challenge the world now faces. Experience gained in this project, however, and in the comparative material with which it provided some familiarity, unfortunately provides little or no information that is helpful in dealing with them.

Copyright National Academy of Sciences. All rights reserved.

Unauthorized Use of Radiation Sources: Measures to Prevent Attacks and Mitigate Consequences

Leonid Bolshov, Rafael Arutyunyan, Elena Melikhova, and Oleg Pavlovsky
Nuclear Safety Institute of the Russian Academy of Sciences

At the beginning of the third millennium, terrorism has become a serious threat to security characterized by its unpredictable nature, variety of forms, and severe effects on the public. Its organizational structures are losing rigid hierarchy and are transforming into international networks consisting of practically invulnerable, independently functioning cells. The terrorists arm themselves with the most recent scientific achievements, adjust civilian technologies to their criminal objectives, and seek to acquire the most destructive and deadly weapons.

The metamorphosis of terrorism into its current form compels all nations to pay attention to problems of terrorism in general and to nuclear terrorism in particular. The notion of a dirty bomb is widely used to mean both a nuclear weapon featuring a low level of technology and a device built with conventional explosives and radioactive substances. The nonproliferation regime and special systems for control and accounting of nuclear weapons predetermine a situation where the threat of the use of radioactive substances for terrorist purposes is the most likely form of terrorism to be carried out.

Radiological terrorism is the deliberate dispersion of radioactive substances, the planting of ionizing radiation sources in the human environs or infrastructure, or acts of sabotage at hazardous radiation facilities, causing radiation impacts on the population and environment and disruption of social life and the economy.

Considering the problem as a whole, one may state that a terrorist act involving radioactive substances of any origin can lead to direct and indirect adverse consequences to society. Direct adverse consequences of radiation effects are

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- acute irradiation of humans by significant radiation doses that within a short period of time (hours or days) results in severe consequences to human health and even fatalities
- prolonged irradiation of humans resulting from environmental contamination with radioactive substances that could trigger long-term adverse radiation effects including an increase in illnesses and fatalities from, for example, cancer

Indirect consequences mean social, economic, political, psychological, and demographic consequences to society, including the following:

- direct damage from a terrorist act leading to possible deaths or serious health effects, radioactive contamination of habitat infrastructure, or loss of property
- costs associated with elimination of the consequences of terrorist acts, required increases in radiation monitoring, deployment of systems for large-scale assessment of the actual radiation situation and its projections for the near and distant future, priority and long-term measures to protect the population, and cleanup of contaminated territories
- degradation of the socioeconomic and psychological situation not only in the regions severely affected by radiation contamination, but also in large territories where small changes in the radiation situation would cause hardly detectable effects to human health and the environment; this would likely trigger population movement from the region and loss of the regional economic potential; frightened people would tend to leave and take their relatives with them from contaminated areas, and the entire way of life for those who stayed behind could also be changed
- costs associated with the withdrawal from the economy of activities in the contaminated territories; possible closure of enterprises; reduction of consumer interest in items being produced in the region regardless of the real contamination levels; devaluation of real estate in the contaminated region; loss of revenues from trade, tourism, and so forth; and decrease in economic attractiveness of the territory
- costs resulting from negative attitudes of the society to radiation in general and nuclear power in particular

Assessments of previous radiation accidents show that the indirect consequences of a radiological terrorism act can lead to economic and social losses that exceed direct losses from radiation impacts on people. In connection with this, serious attention should be paid to potential threats of radiological terrorism acts involving ionizing radiation sources as radiological weapon components. This is due to the wide use of radiation sources in various fields of the economy (industry, agriculture, medicine, and independent power sources; see Table 1)

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 1 Radiation Sources in World Countries

Application	Radionuclide	Half-life	Activity
Radiotherapy	^{60}Co	5.3 yr	50-1,000 TBq
	^{137}Cs	30 yr	500 TBq
Industrial radiography	^{192}Ir	74 days	0.1–5 TBq
	^{60}Co	5.3 yr	0.1–5 TBq
Sterilization	^{60}Co	5.3 yr	0.1–400 PBq
	^{137}Cs	30 yr	0.1-–PBq
	^{90}Sr	29 yr	50–1,500 MBq
Well monitoring	^{137}Cs	30 yr	1–100 GBq
	^{241}Am	432.2 yr	1–800 GBq
Level and thickness gauges	^{60}Co	30 yr	10 GBq–1 TBq
	^{60}Co	5.3 yr	1–10 GBq
Density detector	^{241}Am	432.2 yr	0.1–2 GBq
	^{137}Cs	30 yr	Up to 400 MBq
	^{226}Ra	1,600 yr	Approximately 1,500 MBq

SOURCE: International Atomic Energy Agency. 2003. The Security of Radioactive Sources. Proceedings of an International Conference held in Vienna, Austria, March 10–13, 2003. Vienna: International Atomic Energy Agency.

and imperfections in the system for accounting, licensing, regulating, and control, which make it difficult to bar all paths of illegal movements of ionizing radiation sources, especially in nonnuclear industries.

The Russian Academy of Sciences and the Federal Atomic Energy Agency (Rosatom) have jointly begun work to improve safety in handling radioactive sources, reduce the risk of unauthorized use of sealed radionuclide sources of high activity, and improve the physical protection of radiation sources. Within the framework of this effort, which includes U.S.-Russian cooperation, the Russian Academy of Sciences and Rosatom have started to identify and analyze the physical protection of sealed radioactive sources of high activity and to develop priority measures for improving the state-level system of control, accounting, and physical protection of sealed radioactive sources used in the various sectors of the national economy. Data given in Table 2 and Figure 1 serve as examples of such studies, which characterize the sealed radioactive sources situation in some regions of Russia as of 2004.

As seen from the data given in Table 2, the total number of sealed radioactive sources in a region can vary from a few to several thousand, and in some regions (for example, in Moscow and St. Petersburg) their numbers can be substantially larger. Also, it is important to note that the majority of sources have activity of several curies (see Figure 1) that, on the one hand, reduces the radiological hazard from their use as components of terrorist devices and, on the other hand, leads to the situation where physical security of such radiation sources

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 2 Number of Radioactive Sources in Use in Some Regions of Russia

Region	Quantity	Total activity, Bq
Arkhangelsk Region	3,556	6.15E+16
City of St. Petersburg	18,973	3.93E+16
Kemerovo Region	697	3.57E+15
Samara Region	483	1.24E+15
Saratov Region	1,118	8.04E+14
Khabarovsk Krai	722	9.84E+14
Chelyabinsk Region	5,118	9.13E+15

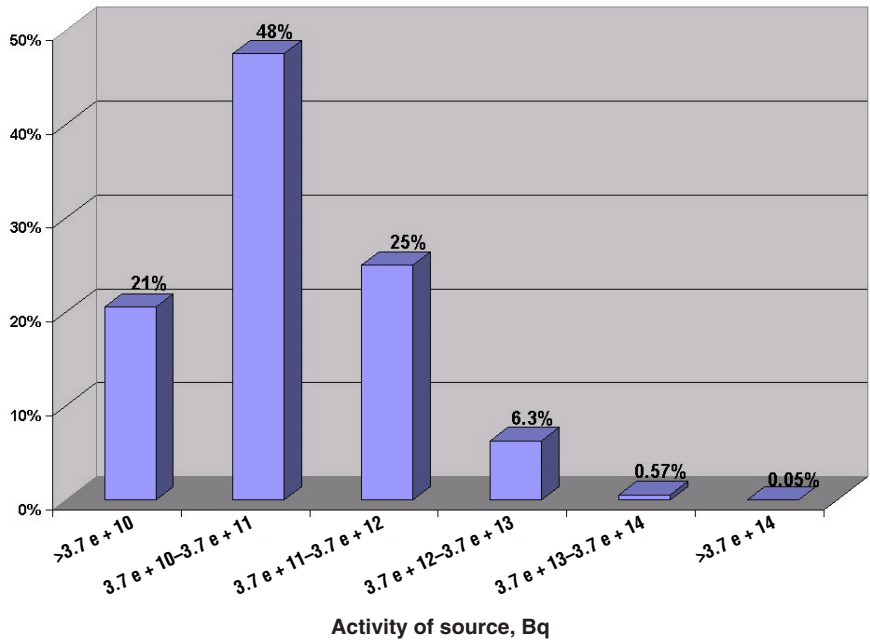


FIGURE 1 Distribution of radioactive sources in use by their activity.

could be much less stringent. Consequently, damage caused by their illegal use can be rather significant since the low-activity sources are much more vulnerable to unauthorized acquisition, clandestine movement, and stockpiling than high-activity sources.

Real difficulties in organizing control and accounting of such ionizing radiation sources can be confirmed by the officially recorded number of detected

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

orphan sources as well as the number of thefts, losses, and damages to sources outside Rosatom's jurisdiction (see Table 3).

Table 3 data show that the most frequent loss of sources takes place in the course of geological surveys where actual control over the security of ionizing radiation sources is extremely difficult. A similar situation is true for other industrially developed countries; for example, in the United States up to 200 radioactive sources are lost annually.

Within the framework of the U.S.-Russian cooperation in improvement of physical protection of nuclear materials, work has included development of recommendations on measures aimed at reducing the possibility of unauthorized use of ionizing radiation sources as based on the analysis of available information. The Brookhaven National Laboratory, acting under a contract with the U.S. Department of Energy, is responsible for this work. At the first stage of the work, a survey of handling conditions for ionizing radiation sources was carried out at enterprises located in 20 regions of Russia (678 organizations) and facilities of 11 federal agencies (676 organizations).

According to the U.S. requirements special attention was paid to the high-activity sources shown in Table 4.

The analysis has shown the number of ionizing radiation sources used in 141 organizations subject to regional jurisdiction and 150 organizations subject to institutional jurisdiction. The number of high-activity ionizing radiation sources is 4,567 and 1,546, respectively.

TABLE 3 Radiological Incidents in Russia Outside the Nuclear Industry Involving Ionizing Radiation Sources from 1997–2001

Incident	1997	1998	1999	2000	2001
Destruction of sources	8	5	6	10	17
Theft of sources	13	22	3	6	6
Detection of orphan sources	14	16	5	1	2
Loss of sources during geological surveys	9	10	14	18	24
Loss of sources during their transportation	—	5	1	2	1

TABLE 4 Minimum Activity Levels for Sources to Be Surveyed

Ionizing radiation	Radionuclides	Minimum activity, Ci
Alpha	^{238}Pu, ^{241}Am, ^{252}Cf, ^{226}Ra	10
Beta	^{90}Sr	100
Gamma	^{60}Co, ^{137}Cs, ^{192}Ir	100

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

A large number of ionizing radiation sources are used by the institutes of the Russian Academy of Sciences. There are 80 such institutes including 15 that possess high-activity sealed radioactive sources (544 are ^{60}Co sources and 69 are ^{137}Cs sources). Many of the sources are no longer in use, and effective measures are required to ensure their security and disposal.

During the analysis, the parameters that characterize handling of sealed radioactive sources were determined, and the basic needs of information and analytical centers were identified in order to implement measures to improve safety in handling sealed radiation sources.

The systems analysis identified three priority areas for reducing threats of unauthorized use of high-activity ionizing radiation sources:

1. disposal of not-in-use ionizing radiation sources to reduce the number of organizations possessing high-activity ionizing radiation sources
2. improvement of the relevant physical protection systems of organizations that handle ionizing radiation sources
3. improvement of the physical protection of ionizing radiation sources during their transportation

A number of factors accounted for the selection of organizations to be classified as first priority in the work plan for reducing the threat of unauthorized use of ionizing radiation sources, including

- the current state of physical protection systems
- security procedures at the facility where ionizing radiation sources are present
- economic and financial stability of the facility
- location of the facility in terms of ease of unauthorized access

Experts from the Nuclear Safety Institute (IBRAE) of the Russian Academy of Sciences, with involvement of specialists from different ministries and agencies of Russia, have carried out for several years system analyses of possible consequences of terrorist acts involving radioactive materials and ionizing radiation sources. An important task of such analyses is to develop approaches to identifying priorities for setting out measures to prevent radiological terrorism acts and minimize consequences. The existing security measures and priorities are based, as a rule, on independent analysis of separate factors such as the design of a dispersion device and its radiation component, a limited set of scenarios of clandestine movements of the dispersion device or its parts, delivery methods to the terrorism scene, and the population affected by the possible consequences of a terrorist act. Regretfully such assessments do not fully take into account the interrelation between health consequences, socioeconomic consequences, and the design of the dispersion device.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

We believe that the probability of radiological terrorism involving a specific type of radioactive substance is determined by

- degree of protection against unauthorized (illegal) removal of the substance
- method of movement into the target area
- availability and effectiveness of detection equipment at different stages of movement and delivery taking into account possible camouflage techniques
- effectiveness of special measures of detecting and terminating preparations for acts of radiological terrorism

In a generalized way, possible combinations of direct and indirect consequences of radiation impacts on humans under various scenarios of radiological terrorism can be divided into the three groups presented in Figure 2. In urban conditions, the situations are most likely to pertain to groups 2 and 3, that is, where indirect consequences prevail as compared to direct radiation consequences for a small group of people at the scene. However, there are scenarios involving a large public presence and possibly significant exposure doses to

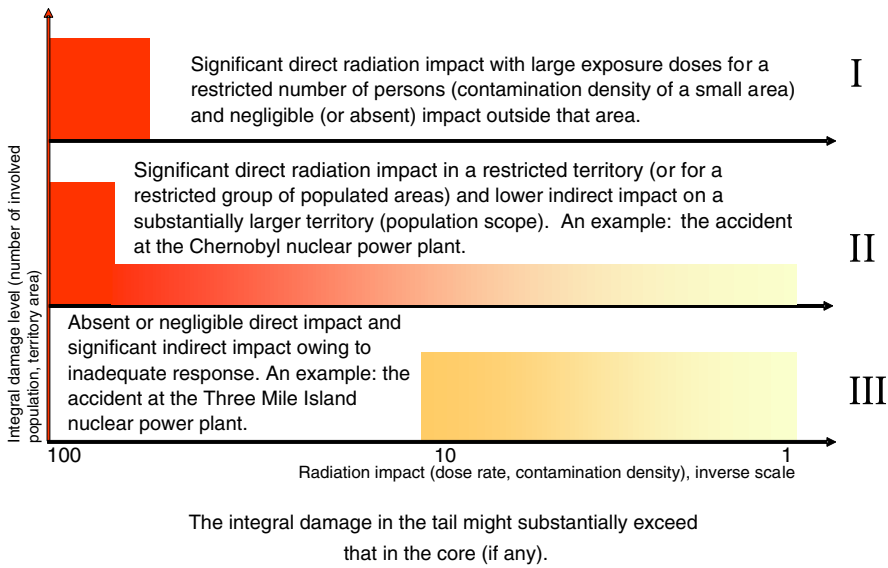


FIGURE 2 Damage caused by different levels of radiation under different scenarios. Note: **I**—high-level radiation impact; **II**—mixed radiation impact; **III**—low-level radiation impact.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

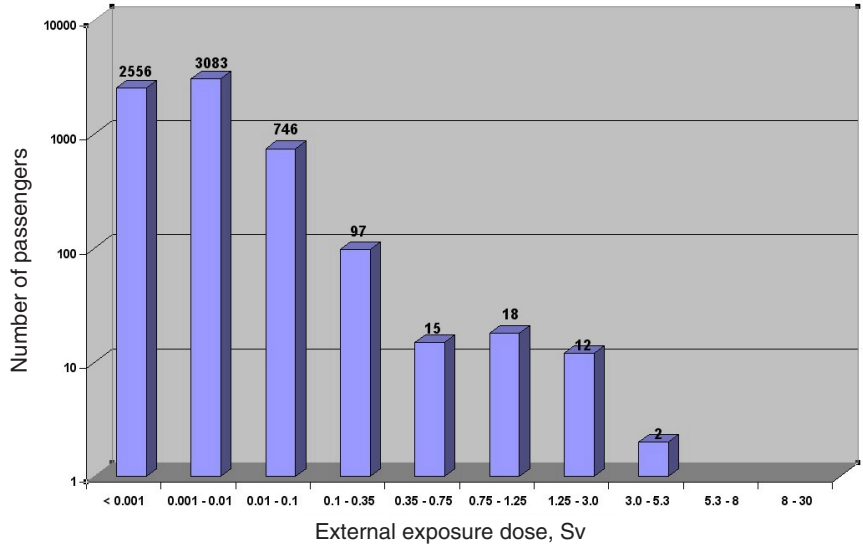


FIGURE 3 Distribution of the subway car passengers by whole-body external exposure doses.

hundreds of people. A summary analysis of the results of assessments of consequences associated with several radiological terrorism scenarios is given below.

The first scenario involves planting a radioactive source containing ^{60}Co in a subway car. Such sources are widely used. The calculations used data for car characteristics, passenger flow, and the length of Moscow's subway system. The calculations have shown that the majority of passengers (nearly 98 percent) could be exposed to external doses below 100 mSv (see Figure 3). About 100–200 passengers could show external signs of a radiation injury (whole-body doses are more than 0.1 Sv and accompanied by a victim's headache, dry mouth, or nausea). For the dozen or so persons who were close to the place where the source had been planted and were exposed to maximum doses, there is even a low probability of death.

The assessments also demonstrate that for a significant number of passengers who were close to the seat where the source had been planted, high-exposure doses to the skin are possible. Such exposure could possibly result in injuries ranging from insignificant reddening to massive fracturing of skin and even internal radiation injuries.

The second scenario concerns the possible consequences of a ^{90}Sr-based dirty bomb detonation at an underground subway station. A shallow subway station layout was selected as the model for this scenario. It was assumed that a low-yield (in TNT equivalent) dirty bomb with a widely used ^{90}Sr radiation

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

source was detonated in the central section of the platform of a subway station during rush hour.

The number of passengers on the platform at the moment of the terrorist act could be up to 1,300 persons, with about 300 persons located in the area close to the detonation. Using conservative assumptions, the maximum internal exposure doses to the lungs of some persons of this group could be 5 Sv. Internal doses of 5 Sv will probably lead to detectable radiation damage to the lungs. For persons receiving exposure doses of about 1–1.5 Sv, the probability of effects is low, but for persons with poor health, especially lung problems, there may be adverse health effects. In addition, the group of passengers may become a high-risk group in terms of possible complementary lung cancer-induced illnesses and fatalities.

The indirect consequences of such a terrorist act will include radioactive contamination of the subway station and adjacent territories from the spread of radioactive substances and closing of the station, and possibly a section of the subway line, for a significant period of time. Simultaneous closing of several stations and transfer stations will nearly immobilize subway operations and cause huge transportation problems. In addition, there will be requirements for compensation for losses of contaminated belongings and for arrangements for long-term medical treatment of a large group of people directly involved in the incident and in the elimination of its consequences.

The third scenario concerns dispersion of some quantity of ^{137}Cs over an urban area. Two ^{137}Cs sources of low and intermediate activity are considered as the sources of radiation. Dispersion of a contaminant at 100 or 200 m above the target area is effected by detonation of a low-yield explosion device or by the use of various dispersion devices.

The assessments used a special code employing Monte Carlo methods and showed that even with dispersion of a low activity ^{137}Cs source over the urban area, there is a probability of 0.2 to 2.6 km^2 of the city being contaminated to higher than 1 Ci/km^2. Larger contamination zones will emerge if a higher activity source is dispersed over the city.

After the Chernobyl accident a contaminated area with ^{137}Cs density of 1–5 Ci/km^2 was identified, according to Russian legislation, as an area of privileged socioeconomic status, although there are no health effects. Application of this guideline to an urban district contaminated as a result of radiological terrorism could lead to mandatory decontamination of an area where thousands of people reside, and losses of apartment and nonresidential buildings could be substantial.

A fourth scenario considers the possible radiological consequences of detonation of a dirty bomb with ^{241}Am radioactivity in or near a large city. It has shown that methodologies and computer codes, which describe the behavior of contaminants when released in an open field or high rugged terrain, cannot be effectively used for urban conditions, large industrial enterprises, and transportation junctions. Therefore a three-dimensional aerodynamic model being de-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

veloped by IBRAE of the distribution of radioactive admixtures in dense urban conditions with identification of typical stagnant areas and local neighborhoods featuring high contamination levels was used. Calculations have shown that an area of substantial contamination of the city environment resulting from such an incident could extend up to 1 km and would be characterized by very high gradients of radioactive concentrations in the air depending on the actual layout of buildings and the weather conditions at the moment of the dirty bomb detonation.

High time and spatial irregularity of the radiation situation parameters causes technical and methodological difficulties in the organization of monitoring and analysis of the radiation situation soon after the act. There is a need to develop special technical means of measurement and computer codes for the processing of monitoring data to obtain adequate estimates of the situation and to outline solutions for population protection.

Preliminary calculations have also demonstrated that about 100 individuals of the 5,000 present in the street at the time of the act could be affected by radiation exposure to the lungs with adverse health effects (over 5 Sv).

The fifth scenario concerns deliberate liquid contamination with high ^{137}Cs concentration of a section of an asphalt road leading to a highway. Contamination of such a section of the road is potentially dangerous because it is the place where vehicles stop before entering the highway and external exposure doses to vehicle passengers increase. Also, the contamination transfer along the highway acquires significance from prolonged contact of car tires with the contaminated road.

Calculations using specially developed models of radioactive contamination transfer have shown that after only 15 minutes from the moment of contamination of the road activities of higher than 100 Ci/km^2 would extend over 100 m. Further along the highway, some cars will exit, and additional roads will be involved in the contamination process. Assessments have shown that within several days after the initial contamination the total length of city roads contaminated over 10 Ci/km^2 could be several dozens of kilometers.

In this case there is no direct radiological impact. Only the road workers and police, who because of their duties remain for several hours in the radiation contamination zone, will receive significant exposure doses. However, indirect losses could turn out to be more significant, since decontamination of large areas of road and sidewalks could be required along with arrangements for alternative traffic routes for extended periods of time. All these operations must take into account rigorous safety guidelines that will lead to labor costs and financial losses.

The radiation anxiety prevailing in the post-Chernobyl period triggered Russia to set forth unjustifiably rigid, legally binding sanitary guidelines. Application of such radiation criteria leads to cases where even only a slight harmless excess over the guidelines becomes a source of serious public concern. In the

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Chernobyl-contaminated area, these have become apparent despite the fact that the allowable exposure level is deliberately lower than variations in natural background radiation.

Inadequate perception of radiation risk exists not only at the level of the average person. Prejudices against radiation are present in nearly all professional and social groups, including representatives of legislative and executive bodies who address public protection and environmental regulatory issues. The work to build adequate perception of threats and possible consequences of acts of radiological terrorism in society requires a differentiated approach to each target group. The information for political and economic decision makers must include not only radiation risk and population protection data, but also data on economic efficiency of these measures, their social acceptability, and their sufficiency.

We may consider the following criteria for zoning territory with radiation impact to the population:

- **Zone 1: radiation impact zone**, which includes territories where radiation effects to the population's health are detected or where emergency criteria are exceeded
- **Zone 2: normal condition guidelines are exceeded**, including human exposure limits for normal conditions, environment contamination levels based on sanitary and ecological criteria, external dose rates related to natural background values, and accepted contamination levels for accidents
- **Zone 3: socioeconomic consequences**, where social and economic conditions are disrupted and the population's radiation concerns are clearly manifested

As a rule, in all of the radiological terrorism scenarios in an urban area, the size of low-contaminated sections (Zones 2 and 3) can exceed by 100 and more times the size of severely contaminated ones (Zone 1). This ratio turns out to be somewhat less in the Chernobyl area in Russia, due to a large number of rural settlements in these zones.

Actual measurement data demonstrate the high irregularity of contamination densities and dose rates of gamma radiation in residential parts of the Chernobyl area. There are also great differences in individual exposure doses in various professional groups and age groups. All these factors complicate territorial zoning, build negative attitudes of the population toward protective measures, and aggravate social tension. Analysis of the radiological terrorism scenarios shows that these problems will be more difficult to solve in urban conditions.

The fear of radiation and the rigidity and confusing nature of existing guidelines and criteria in the field of radiation safety and radiation protection make society extremely vulnerable to a radiological terrorism threat. This fear, in combination with the ease in acquiring instruments capable of detecting the slightest increases of the radiation level, makes the system as a whole substantially un-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

stable. Social risk amplification mechanisms are triggered by the slightest threat of a terrorist act involving radiation sources. In these cases the magnitude of indirect damage caused by fear-induced behavioral responses will inevitably exceed any consequences of radiation exposure itself. The epidemic of fear can spread extremely fast in densely populated areas with well-developed communications while endangering the entire system of societal activities.

Why does society demonstrate such an inadequate response to radiation hazards? The fear of radiation has historic and psychological roots. The mere term *radiation* inevitably evokes in the vast majority of people the association with nuclear weapons and is accompanied by the vision of the atomic bombing of Hiroshima and Nagasaki. These images were implanted intensely in people's minds during the years of the arms race. The second layer of negative associations is represented by the Chernobyl, Kyshtym, and other radiation accidents. This sequel of radiation disasters with thousands of imaginary victims of peaceful applications of the atom has been ingrained in the mass consciousness.

Public addresses of officials from affected countries—Belarus, Ukraine, and often Russia—have also contributed to public confusion. Huge economic losses due to the Chernobyl accident, thousands of square kilometers of contaminated soil, and millions of people who needed help were and are cited in all programmatic documents on Chernobyl used to emphasize the large-scale measures being taken to rehabilitate the area, especially when the accident consequences are discussed at the international level. This distorted image of radiation accidents of the past will certainly become a serious negative background for discussions of actual or projected consequences of radiological terrorism.

For the subsequent comparative assessments of the scale of social consequences of radiological terrorism, we introduce two categories of people—involved and concerned—in addition to the traditionally used categories of exposed and affected.

The involved category includes those who witnessed the event but whose radiation dose resulting from a radiological terrorism act does not exceed guidelines for normal conditions. For example, for detonation of a dirty bomb in the subway, the involved would be all passengers of cars present at the station at the moment of the blast. In the scenario of the detonation on the street, the involved would be residents of buildings subject to evacuation or decontamination who were in their homes at the time of the terrorist act. The involved will think they have strong grounds to be concerned about their health, since according to the linear nonthreshold model of radiation biological effects adopted by International Commission on Radiological Protection, any arbitrary low-exposure dose can lead to adverse consequences to health.

The concerned category may be the persons who received negligibly low (close to zero) additional doses, but their standards of living dropped because of the terrorist act. They could be residents of buildings neighboring the evacuation zone, families of exposed individuals, colleagues who are afraid of catching the

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

disease during contact with the exposed individuals in the office, residents of the location where repositories of radioactive waste resulting from demolition and decontamination could be located, and so forth.

Those in the concerned category, the same way as those in the involved category, have formal grounds (the linear nonthreshold hypothesis) to believe that their health could have been damaged. Past accident experience demonstrates that the number of concerned will be 2–3 orders of magnitude higher than those involved. If there is a terrorist act in the center of a megapolis, the number of concerned could approach several million people. The scale of sociopsychological consequences in many respects is determined by the massive nature of the phenomenon of being concerned. At an early stage these consequences are manifested in the form of distress, behavioral responses of self-defense, and mental disorders. They cannot be expressed in terms of money, but under certain circumstances these side effects could be as significant as the economic losses expressed in terms of money. As time passes the external manifestations of distress and social disadaptation decline, but distrust of the authorities and negative attitudes toward nuclear technologies remain. Lessons learned from the accidents of the past show that the aggravation of already existing social problems and politicization of the society take place in radiation-contaminated territories.

We may judge the scale of social response and rumor-spreading speed even without a radioactive substance release by the recent public response to the operational event at the Balakovo Nuclear Power Plant in Russia. The event occurred at night on November 4, 2004. It was rated Level 0, that is, without a radioactivity release, by the International Nuclear Events Scale (INES); but it indeed produced rumors in the plant's satellite city of Balakovo (due to the lack of adequate official information) about an accident with a release of radiation. Relatives and acquaintances started telephoning each other, recommending that they immediately drink iodine and wine and, if possible, leave the area. In 30 hours, millions of residents of the European part of Russia, who can be attributed to the category of the concerned, were involved in the situation. A few cases of iodine poisoning were reported as a result of the panic.

At all levels of response to the radiation threat, there is so-called social risk amplification, which leads to great growth in the scale of indirect losses. This is confirmed by the experience of past radiation accidents. For example, after the accident at Chernobyl, protective measures were justified (proceeding from the radiation protection criteria under conditions existing at that time) for 300,000 persons. In fact, more than 7 million persons were covered by the intervention measures. Different estimates of the cumulative economic loss (direct losses plus indirect damage) varied from tens to hundreds of millions of U.S. dollars over 15 years after the Chernobyl catastrophe for Belarus, Russia, and Ukraine. If one is being guided by the Nuclear Energy Agency (NEA) estimates (2002), in the event of a hypothetical accident at a modern nuclear power plant, the consid-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

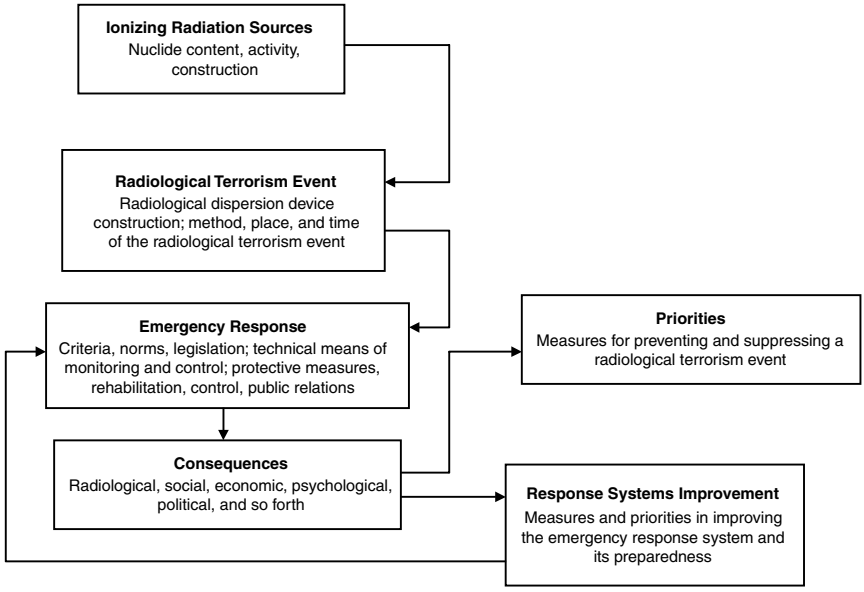


FIGURE 4 Factors determining radiological terrorism consequences and their interrelation.

eration of social risk amplification would boost losses caused by such an accident from EUR 10–20 billion up to nearly EUR 400 billion.

The mechanism for working out measures and setting priorities to prevent, terminate, and minimize consequences of radiological terrorism acts can be represented, with some simplifications, in the form of the diagram shown in Figure 4. Outlining effective measures and priorities requires a systems approach based on the multiattribute analysis of

- various scenarios of illegal acquisition and paths of radioactive substance movements, taking into account their camouflage from detection equipment, especially for alpha and beta emitters
- possible designs of dispersion devices, and paths and targets for terrorist acts
- a whole set of consequences (radiological, ecological, sanitary and hygienic, economic, social, and so forth), taking into account features of radiation situations under different scenarios of radiological terrorism in urban conditions (for example, short timeframe for occurrence, special irregularity of urban radioactive contamination, multifaceted infrastructure)
- requirements for methodologies and equipment for radiation survey and

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

monitoring including achievable detection levels of alpha, beta, and gamma radiation during illegal movements of radioactive substances, considering camouflage capabilities and means of movement and delivery

- the existing legal and regulatory bases in the field of radiation safety and the effects on decision making
- practical applicability of radiation protection criteria for the population, taking into account the high irregularity of radioactive contamination, complex distribution of individual exposure dose, and many interrelated components of urban infrastructure
- causes of inadequate public perception of radiation risks

The development of instrumental means of countering radiological terrorism must pursue two paths:

1. strengthening of control over possible movements of radioactive sources, especially in public places and critical facilities of the city
2. development of methods for radiation surveys in urban conditions, including at critical infrastructure objects, life support systems, and public places, and for designing the most effective measures to protect the population

In this regard the following operations are needed immediately:

- creation of hardware and software for control and prevention of carrying and conveying radioactive substances into public places or critical facilities of the city
- development of methods and hardware and software sets for radiation surveys in urban conditions
- development of decision-making support systems for adequate countermeasures for public protection in the event of a terrorist act involving radioactive substances

Stationary and mobile equipment for monitoring and surveying the radiation situation must ensure accurate and complete input information and prompt transmission and processing of data for large numbers of radioactively contaminated objects within the limited time for decision making.

Requirements for the equipment for detection of illicit trafficking of radioactive substances, their control and accounting systems, and special termination measures must be based on a realistic assessment of dangerous quantities of various radionuclides (especially alpha and beta emitters), as derived from the analysis of potential radiological, sanitary and hygienic, social, and economic consequences of the radioactive substance that is used.

Regretfully the existing radiation monitoring systems of large cities are not capable of detecting high radiation contamination or identifying gamma-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

emitting ionizing radiation sources entering the city by criminal methods. This can be demonstrated using the example of Moscow. At present there are about 150 automatic radiation survey stations (ARMS detectors). Taking into account the city's area (1,081 km^2), the average survey zone of such a station is about 7 km^2, or 1.5 km in radius.

Simple calculations show that when standard ARMS equipment is used, the detection of significant quantities of gamma-emitter activities is limited by a 100 m zone when the source is in the direct sight of the detector or has poor radiation shielding. The detection task becomes more difficult with alpha and beta emitters and requires special equipment. In essence the detection of radioactive substances is limited to simple tasks, such as monitoring separate critical zones where radioactive substances are moved without authorization. The setting of an effective system for detection of unauthorized movement of radioactive substances is far from being solved.

Special radiation monitoring methods should be developed and introduced to address these objectives. The prompt (within several seconds) detection of a moving ionizing radiation source requires a statistically verified detector with counting speed over the background; that is, at the background counting speed of about 1 pulse, the counting should be approximately double that. Therefore, the natural threshold of detection of a gamma source by standards instruments is 10 μR/h. Sensitivity of detectors can be increased by enlarging the detector volume and extending the measurement time. In this case, however, the cost and size of instruments will increase significantly. In addition stability and reliability will become difficult for large or multidetector equipment.

The significant reduction of signal/noise ratio can also be achieved through measurements in the spectral mode when the source radiation is recorded in the preset energy range (certainly, this range must be known in advance and preset) or through the use of a collimator. Both approaches require long exposure times (10 seconds to 1 minute), but they allow for increasing sensitivity by an order of magnitude and higher (see Table 5).

Yantar radiation monitors (designed by the Aspekt Company) are examples of existing stationary radiation source search equipment. Yantar monitors are designed to detect radioactive and fissile materials in the course of automated monitoring of vehicles, luggage, and people. Stationary radiation monitoring posts are furnished with such systems. There are several makes of Yantar monitors: pedestrian, vehicle, railway, and mail-luggage monitors. Yantar monitors have an independent alarm archive, well-developed self-diagnostics, and remote access capabilities for the setup parameters and alarm archive of the monitor.

Granat portable concealed radiation monitors (also designed by Aspekt) are an example of equipment that has already been developed. The monitor is designed to detect radioactive and fissile materials and primary identification of gamma-emitting radionuclides. Granat monitors can be used for radiation monitoring at temporary checkpoints (for example, ship's ladders and entrance check-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 5 Capabilities of Ionizing Radiation Sources Detection Complex with a Collimator's Angle Resolution of 20° (developed by ETC of the Khlopin Radium Institute, St. Petersburg)

	Distance, m			
	One rotation of collimator (6 s)		10 rotations of collimator (1 min)	
Source and its activity	By integral counting	By photopeak	By integral counting	By photopeak
^{137}Cs, 1.2 GBq	70	85	110	150
^{60}Co, 4.1 GBq	110	140	160	220

points in recreation facilities), for equipping special service officers to carry out concealed radiation monitoring, and so forth. Granat monitors record gamma radiation using NaI(Tl) crystal-based scintillation detectors and neutron radiation using proportional ^{3}He counters.

Since cities are the likely targets of radiological terrorism acts, the existing methods of radiation survey and interpretation of measurement results could turn out to be only partially adequate. In addition, the existing methods and systems of emergency response to radiation accidents also could not produce adequate results in the event of a terrorist act, in the first place, because of the necessity to respond and make decisions immediately.

It means that it is necessary to develop new methods of calculation, modeling, measurement, and analysis of radioactive contamination in large cities' conditions. Besides, in densely populated cities the development of operative and highly effective systems for support of decision making based on state-of-the-art means of communications and monitoring techniques becomes ever more important. A number of priority tasks may be identified:

- the development of requirements for equipment and organization of a system for detection of illegal movements of radioactive substances, based on an analysis of potential consequences of their use and method of their delivery to the radiological terrorism scene
- the development and manufacture of corresponding detection equipment
- the creation of the corresponding methodological basis, software and hardware support, and system for expert support of decision making regarding population protection
- the generation of recommendations for a regulatory basis in the field of

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

radiation safety, which will ensure effective protection of human health and prevention of unjustified social and economic consequences

- the development of a methodology and equipment for radiation survey and monitoring in large cities
- the establishment of national specialized centers for expert support of decision making regarding protection of the population and territories in the event of radiological terrorism
- the development of a strategy and establishment of a corresponding system for emergency response and protection of population and territories in the event of radiological terrorism
- the establishment of national and international systems to objectively inform the public about radiation risks, radiation safety approaches and guidelines, and lessons learned from radiation accidents and incidents of the past

To address the radiological terrorism issue, the implementation of work in these areas should be backed up by the best practices of U.S.-Russian cooperation in the field of radiation safety and protection. This will allow for finding ways to reduce the probability of radiological terrorism acts and to minimize their direct and indirect consequences should they occur.

Copyright National Academy of Sciences. All rights reserved.

Other Dimensions of Radiological Terrorism

John F. Ahearne
Sigma Xi, The Scientific Research Society

An examination of possible threats to the United States and Russia begins with the conclusion that there are groups in the world who would like to destroy these countries or, at least, topple their governments. Russia has experienced a number of terrorist attacks such as the hostage taking in a Moscow theater, suicide bombers on airplanes, and the horrific siege of a school full of children. The United States has experienced the September 11, 2001, terrorist attacks.

A 2002 National Academies study, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*,[1] grouped nuclear and radiological threats into three categories:

1. stolen state-owned nuclear weapons or weapons components, modified as necessary to permit terrorist use
2. improvised nuclear devices (INDs) fabricated from stolen or diverted special nuclear material (SNM)—plutonium and, especially, highly enriched uranium (HEU)
3. attacks on nuclear reactors or spent nuclear fuel or attacks involving radiological devices

For these categories, that report provided matrices of the threat, risk (probability and consequence), and policy issues, shown in Table 1.

[1]NRC Committee on Science and Technology for Countering Terrorism. 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 1 The Nuclear and Radiological Threat Matrix

TABLE 1-A State-owned Nuclear Weapons

Threat Category	Threat Description	Threat Level
State-owned nuclear weapons	Theft and diversion of state-owned nuclear weapons for use, with or without modification, against U.S. targets or assets	United States: Low—weapons are well protected and tactical weapons have integrated permissive action links to prevent unauthorized use
		Britain, China, France, Israel: Low—weapons are few in number relative to U.S.-Russian arsenals and are well protected
		Pakistan, India: Medium—weapons are under secure control of the military, but political situation is unstable
		Russia: Medium—large numbers of weapons with poor inventory controls

A recent book[2] added radioactive sources to this list and described what the authors called the four faces of nuclear terrorism, as follows:

1. the theft and detonation of an intact nuclear weapon
2. the theft or purchase of fissile material leading to the fabrication and detonation of a crude nuclear weapon—an IND
3. attacks against and sabotage of nuclear facilities, in particular nuclear power plants, causing the release of large amounts of radiation

[2]Ferguson, C., W. Potter, A. Sands, L. Spector, and F. Wehling. 2004. The Four Faces of Nuclear Terrorism. Monterey, CA: Center for Nonproliferation Studies, Monterey Institute of International Studies.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Potential Consequences	Probability of Occurrence	Technical and Policy Changes	Approaches to Mitigation
Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Moderate over the next five years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected if theft occurs in Russia	Improve indications and warnings capabilities
		Stolen or diverted weapons could be converted for terrorist use	Improve security of Russian and Pakistani nuclear weapons at storage sites and borders
		HEU-based weapons smuggled into the United States could be difficult to detect and recover	Accelerate deployment of sensor arrays at critical U.S. entry points and targets
		First responders may be killed or incapacitated by attack	Develop and announce policies to deter use of weapons by terrorist states
			Improve attribution capabilities

4. the unauthorized acquisition of radioactive materials contributing to the fabrication and detonation of a radiological dispersion device (RDD)—a dirty bomb—or radiation emission device (RED)

The authors of this book wrote, "The United States has faced the threat of nuclear terrorism for many years, but this peril looms larger today than ever before."[3]

Finally, at the Workshop on Terrorism in a High-Tech Society and Modern Methods for Prevention and Response in 2001, the following was presented from the Russian viewpoint:

[3]Ibid., p. 1.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 1-B Improved Nuclear Devices

Threat Category	Threat Description	Threat Level
Improvised nuclear devices	Theft or diversion of SNM for fabrication of nuclear devices for use against U.S. targets or assets	United States: Low—SNM is well protected
		Britain, China, France, India, Israel, Pakistan: Low—small amounts of materials are well protected
		Russia: High—large inventories of SNM are stored at many sites that apparently lack inventory control, and indigenous threats have increased

SOURCE: NRC Committee on Science and Technology for Countering Terrorism. 2002. Pp. 42–47 in Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Potential Consequences	Probability of Occurrence	Technical and Policy Changes	Approaches to Mitigation
Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Moderate over the next five years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected	Improve indications and warnings capabilities
		Crude HEU weapons could be fabricated without state assistance	Consolidate SNM at Russian sites, improve inventory controls, and improve security at sites and borders
		HEU-based INDs smuggled into the United States could be difficult to detect and recover	Accelerate blend-down of Russian HEU
		First responders may be killed or incapacitated by attack	Accelerate the development and deployment of SNM sensor arrays at critical U.S. entry points and targets
			Improve capabilities for remote detection of HEU
			Develop and announce policies to deter use of INDs by terrorist states
			Improve attribution capabilities

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Terrorist acts using sources of radiation may be divided into three categories:

1. the detonation of (or threat to detonate) either a nuclear explosive device stolen from storage arsenals or a homemade nuclear bomb device using highly enriched uranium or plutonium
2. the theft of radioactive waste material and similar substances from nuclear facilities such as atomic power stations, research reactors, irradiated fuel processing plants, and storage facilities
3. the detonation of an ordinary explosive device including radioactive isotopes as one of its components (^{60}Co, ^{90}Sr, ^{137}Cs, ^{239}Pu, and so forth), with the aim of subsequently dispersing them over significant areas; this category would also include the possible addition of radioactive substances to water systems[4]

NUCLEAR BOMBS

The National Commission on Terrorist Attacks Upon the United States wrote the following:

> The greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons. [We note that] al Qaeda has tried to acquire or make nuclear weapons for at least ten years.[5]

The greatest concern is an actual nuclear bomb. A bomb is not necessarily a nuclear weapon, which implies a device designed to be used in warfare, mounted on an airplane, in a missile, or used in a torpedo or landmine. A nuclear bomb is a device than can result in a nuclear explosion. India exploded a "peaceful" device in May 1974. Of course, theft of a real weapon could be disastrous, *if* the thieves knew how to set it off. This is not particularly easy and may be impossible unless the thieves included insiders.

Whereas there is serious concern about radiological sources, especially for high dose-rate sources hidden in congested areas, use of a nuclear device would be catastrophic. This could be delivered using the current delivery system of choice—a truck bomb. Another delivery system would be on a ship berthed in a city's harbor.

How could such a nuclear device be made? As stated by the NRC Committee on Upgrading Russian Capabilities to Secure Plutonium and Highly Enriched Uranium, "A major technical impediment confronting a nation or group bent on

[4]Bolshov, L., R. Arutynyan, and O. Pavlovsky. 2002. Pp. 137–138 in High-Impact Terrorism: Proceedings of a Russian-American Workshop. Washington, D.C.: National Academy Press.

[5]National Commission on Terrorist Attacks Upon the United States. 2004. P. 380 in The 9/11 Commission Report. New York: W. W. Norton and Company.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

developing nuclear weapons is the difficulty of obtaining the necessary direct-use material. A minimum of a few kilograms of plutonium or several times that amount of highly enriched uranium (HEU) is required, with the quantity depending on the composition of the material, type of weapon, and sophistication of the design."[6]

To make a nuclear device, one needs fissile material, either highly enriched uranium or plutonium (Pu). The amount for an explosion is related to the critical mass needed for the chain reaction that is the explosion. This "is about 10 kilograms for plutonium-239 and about 60 kilograms for uranium-235, when these materials are in the form of metal spheres at their normal density. In nuclear weapons, these values might be reduced by a factor of 4 if the force of a powerful explosive is sufficient to double the density of the plutonium by compression. . . ."[7]

Although much less material is needed, plutonium devices are harder to make and plutonium is harder to obtain. It is not naturally occurring, but must be produced in neutron irradiation of uranium followed by chemical separation of the plutonium, that is, reprocessing of the irradiated uranium. This requirement makes it unlikely to be constructed by a subnational group. Also, once made, it is radioactive and therefore not easily hidden from inspections or surveillance.

However, uncomfortably large amounts of plutonium from the reprocessing of spent fuel exist in several countries, such as Russia. Although this plutonium is not weapons grade but reactor grade, it is quite adequate to make a nuclear weapon. "[I]t would be quite possible for a potential proliferator to make a nuclear explosive from reactor-grade plutonium using a simple design that would be assured of having a yield in the range of one to a few kilotons, and more using an advanced design."[8]

HEU weapons are easier to construct. The key factor is obtaining the fissionable material. HEU is made by reducing the amount of nonfissionable uranium in naturally occurring uranium. Enrichment technology is well known, although it is advanced technology. While it may be difficult to obtain HEU, the Pakistan nuclear designer A. Q. Khan apparently widely spread the knowledge and technology. It still is not easy for a nonnational group to obtain enrichment technology. However, there is another route to obtain HEU: steal or divert it from a research reactor, many of which are fueled with HEU. The United States and Russia, as well as many other countries, have such research reactors, which are a growing nonproliferation concern.[9]

---

[6]Committee on Upgrading Russian Capabilities to Secure Plutonium and Highly Enriched Uranium. 1999. P. 1 in Protecting Nuclear Weapons Materials in Russia. Washington, D.C.: National Academy Press.

[7]Garwin, R. L., and G. Charpak. 2001. P. 34 in Megawatts and Megatons. New York: Knopf.

[8]Committee on International Security and Arms Control. 1994. P. 33 in Management and Disposition of Excess Weapons Plutonium. Washington, D.C.: National Academy Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

In one of a series of articles on threats, a reporter for *The Washington Post* wrote, "Nuclear scientists tend to believe the most plausible route for terrorists would be to build a crude device using stolen uranium from the former Soviet Union. Counterterrorism officials think Bin Laden would prefer to buy a ready-made weapon stolen in Russia or Pakistan and to obtain inside help in detonating it."[10]

ACCESS TO SPECIAL NUCLEAR MATERIAL

In discussing the future threats to the United States, the National Commission on Terrorist Attacks Upon the United States wrote, "A complex international terrorist operation aimed at launching a catastrophic attack cannot be mounted by just anyone in any place. Such operations appear to require [among many factors] . . . access, in the case of certain weapons, to the special materials for a nuclear, chemical, radiological, or biological attack. . . "[11]

Keeping HEU and plutonium out of the hands of terrorists is the most important action in protecting against use of nuclear devices by such groups. This requires protection of materials at the storage locations, tracking of materials when in transit, and an accounting system that enables authorities to verify amounts at locations. Both Russia and the United States have devoted efforts to improve the materials protection, control, and accounting (MPC&A) systems in Russia, with the United States having contributed hundreds of millions of dollars to upgrade security at locations where HEU and plutonium are stored.

There continue to be concerns about a black market for these materials, with periodic reports of small amounts being found by inspectors. In a 2003 workshop, a Russian official wrote, "A fundamental component in the creation of a state system for countering the illegal circulation of radioactive material is the development of devices for their detection, location, and identification and the provision of such instruments to the structural components of the system."[12]

There are other very significant amounts of radioactive materials in the United States and Russia.[13] Both countries have large quantities of spent nuclear

---

[9]NRC Committee on End Points for Spent Nuclear Fuel and High-Level Radioactive Waste in Russia and the United States. 2003. End Points for Spent Nuclear Fuel and High-Level Radioactive Waste in Russia and the United States. Washington, D.C.: The National Academies Press.

[10]The Washington Post. Linzer, D. December 28, 2004. Nuclear Capabilities May Elude Terrorists, Experts Say.

[11]National Commission on Terrorist Attacks Upon the United States. 2004. Pp. 366–367 in The 9/11 Commission Report. New York: W. W. Norton and Company.

[12]Kutsenko, V. M. 2004. International Aspects of Creating a State System for Countering the Illegal Circulation of Radioactive Materials in the Russian Federation. P. 161 in Terrorism—Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

fuel, that is, fuel removed from reactors after useful fuel life. This spent nuclear fuel is highly radioactive and thus might be seen as a potential material to be used with conventional explosives to construct an improvised radiological device, or dirty bomb. The amounts of such material are vast, but the difficulties of using it are also large because of the intense radiation field associated with spent fuel. Similarly, liquid and, in some cases, solid radioactive wastes are also stored in large amounts in the United States and Russia. Waste is unlikely the material of choice for a device due to difficulty of access, radiation fields associated with the waste storage areas, and difficulty of using it in a device. However, such storage areas do present targets for explosive dispersal.

The U.S. Nuclear Regulatory Commission has increased the design basis threat against which U.S. nuclear power plant operators are required to defend. The Department of Energy (DOE) also has increased the design basis threat against which DOE nuclear laboratories and other nuclear facilities must defend.

CONCLUSIONS

In all these cases, including radiological sources and so-called dirty bombs, the words *nuclear* and *radioactive* can cause fear and, if stressed enough, panic. The fear associated with these words is hard to counter. It has been called *radiophobia*,[14] and "it is generally agreed that the greatest consequences of an RDD are public fear and the potentially enormous cleanup costs along with the consequent economic losses."[15]

The U.S. National Academies and the Russian Academy of Sciences have worked together for a half-century.[16] There is no issue more important for these two institutions than to continue mutual efforts on nonproliferation, including efforts to reduce the threats of radiological terrorism.

[13]NRC Committee on End Points for Spent Nuclear Fuel and High-Level Radioactive Waste in Russia and the United States. 2003. End Points for Spent Nuclear Fuel and High-Level Radioactive Waste in Russia and the United States. Washington, D.C.: The National Academies Press.

[14]Bolshov, et al., op. cit., p. 137.

[15]Hecker, S. S. 2002. Nuclear Terrorism. P. 151 in High-Impact Terrorism: Proceedings of a Russian-American Workshop. Washington, D.C.: National Academy Press.

[16]Schweitzer, G. E. 2004. Scientists, Engineers, and Track-Two Diplomacy: A Half-Century of U.S.-Russian Interacademy Cooperation. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Biological Terrorism: Regional Preparedness[1]

Russ Zajtchuk
Chicago Hospitals International

INTRODUCTION

The limitation and eventual elimination of chemical and biological weapons are two of the greatest challenges facing the international community in this century. Unfortunately, proliferation of capabilities to construct such weapons is continuing despite the best efforts to contain such technologies by many nations, including the United States.

Biological terrorism, in particular, is of great concern for several reasons:

- Many potent agents are readily available. Theoretically, any microorganism or toxin capable of inflicting death or disease has the potential of being adapted for use as a biological weapon.
- Naturally occurring infectious agents could be used to generate epidemics among susceptible populations, creating confusing disease situations. Naturally occurring or deliberately disseminated spore-forming microbes might continue to persist in the environment, and some aerosolization might occur; environmental detectors might not be able to differentiate between natural and artificially generated contamination.
- Many classic agents of concern can be mass produced in a short time by using basic laboratory techniques. Large fermenters may not be necessary if a small amount of agent is all that is required.

[1]Editor's Note: This paper was presented before the natural disasters in 2005 in the United States and thus does not incorporate the lessons learned from those events.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- Theoretically, biological agents can be genetically altered to escape detection.
- Dangerous biological agents require no precursors for development, unlike chemical and nuclear agents, and a covert program is much more difficult to detect.

Before 1990 little thought was given to the possibility of a biological terrorist attack on U.S. cities. Even as recently as 1997, the U.S. Department of Defense spent only $137 million on biodefense to protect the deployed force, while academia, industry, local governments, and the rest of the federal government were in some cases doubtful about the threat of biological terrorism.

Since fiscal year 2000, the United States has committed billions of dollars to military biodefense and to domestic preparedness for biological attack. The federal government has formed the U.S. Department of Homeland Security, a number of university medical centers have received funding for developing research programs in biodefense, and state and local governments have become proactive in developing and implementing emergency preparedness and disaster response plans to counter terrorism.

REGIONAL PREPAREDNESS

At the request of the Illinois Department of Public Health, a proposal was developed primarily by the University of Illinois for a statewide bioterrorism plan. In 2002 a number of leading universities were designated as Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases by the National Institute of Allergy and Infectious Diseases (NIAID), one of the National Institutes of Health,[2] and charged to develop emergency preparedness and disaster response plans. The first year focused on needs assessments and planning activities. The centers of excellence coordinated the needs assessments for nongovernmental health care entities. Upon completion of assessments, the health care entities and the Illinois Department of Public Health received reports on their emergency and terrorism preparedness.

With the assistance of centers of excellence and the Illinois Department of Public Health, all health care entities developed uniform clinical protocols for clinical interventions for biological, chemical, radiological, nuclear, and explosive acts of terrorism. They developed a syndromic round-the-clock surveillance system in Illinois for uniform reporting of diseases from hospital emergency departments to the Illinois Department of Public Health. Finally they integrated

[2]For more information about the National Institute of Allergy and Infectious Diseases (NIAID) Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases program, see http://www.rcebiodefense.org/ and http://www3.niaid.nih.gov/Biodefense/Research/rce.htm#map.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

surveillance with a statewide laboratory network for testing and reporting of results.

A General Accounting Office (GAO) report in August 2003[3] indicated that hospitals do not have surge capacity to support a large-scale terrorist event. Consequently steps have been taken to develop a plan to accommodate at least 1,700 patients in an emergency. Additionally an emergency system was developed to increase staffing levels in acute care hospitals during a major event and to develop a cadre of reserve health care personnel by reaching out to retired practitioners, nurses, and health care students and by providing education to the public to further emergency preparedness.

Resources were allocated to obtain a self-contained, fully equipped mobile medical facility with a capacity for 100 beds, including 30 intensive care, 24 ambulatory, and 46 acute care beds. Staffed by personnel from 31 acute care hospitals and state governmental agencies, it has the potential to be used in any location across the state because of mobility and has the capability to provide isolation care for any type of infectious disease, including smallpox. This mobile hospital is being used to enhance emergency preparedness through training, drills, and exercises.

Communication systems were assessed. A communitywide and statewide communication strategy and plan for round-the-clock availability, interoperability, and redundant capacity was developed. Additionally, each of the acute care hospitals installed MEDSAT satellite phones and developed protocols for their utilization.

After coordinating with state and local public health and health care delivery entities on stockpiling equipment, supplies, vaccines, and pharmaceuticals, a uniform plan was developed for the distribution of stockpiles. Administrators in acute care hospitals received orientation and training on how to procure, track, and deliver strategic national stockpile supplies.

The statewide laboratory system's capabilities were assessed and communication capabilities between laboratories and health care providers were evaluated. Health care facilities have been asked to address the following:

- HVAC/high-efficiency particulate arrestance filtration
- water systems
- security/lockdown
- isolation rooms
- decontamination equipment
- personal protection equipment

[3]U.S. General Accounting Office. 2003. Hospital Preparedness: Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response. Report to Congressional Committees GAO-03-924. Washington, D.C.: U.S. General Accounting Office. In July 2004 the General Accounting Office became the Government Accountability Office.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- radiation detection equipment
- chemical detection equipment

Additional information on statewide regional preparedness may be obtained from the Yale New Haven Center for Emergency Preparedness and Disaster Response, Yale School of Medicine.[4] The center has an emergency management course on CD-ROM.

INFORMATION ANALYSIS CENTER FOR HOMELAND SECURITY AND MEDICAL RESPONSE

There is a wealth of information on homeland security and medical response with different areas of expertise ranging from clinical protocols to logistical solutions. However, this information is not systematized or easy to locate, access, evaluate, and implement. National defense organizations and other government and civilian groups are mandated to implement emergency preparedness and disaster response programs. To maximize their effectiveness, these groups need resources to help them identify the most accurate, comprehensive, and current information available on homeland security and medical response topics, whether from a military or civilian, public or private, or domestic or international source. Best practices already developed and successfully implemented for homeland security and medical response need to be assessed, adapted, and disseminated to a broader audience.

Formation of an Information Analysis Center (IAC) for Homeland Security and Medical Response is to be that resource. The significance and power of the IAC will be derived from the partnership of diverse groups, each of which has resources and expertise that the others cannot now access in a coordinated way. The groups include military and civilian, public and private, and domestic and international organizations. Groups engaged in homeland security and medical response will benefit from having access to sources of information previously unavailable to them. Prime examples include making available to civilian groups' information on biological and chemical threat agents and emergency response drills and exercises conducted by the military. The IAC will facilitate application of existing homeland security and medical response solutions with demonstrable capabilities, nonduplication of financial and other resources, and maximum return on investment for governmental and private funding sources, supporting uniform coordinated national preparedness and response.

An IAC has been established for use by Rush-Presbyterian-St. Luke's Medi-

[4]For additional information, contact: Yale New Haven Center for Emergency Preparedness and Disaster Response, 1 Church Street, 5th Floor, New Haven, CT 06510, Telephone: (203) 688-3224, Fax: (203) 688-4618, E-mail: center@ynhh.org; Web site: http://www.ynhhs.org/emergency/index.html.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

cal Center in the field of telemedicine, and another IAC has been created for use by the U.S. Department of Defense. Both IACs may be accessed by the public through the institutions' Web sites. In addition, plans are being developed to establish a regional IAC for the Chicago area.

Areas of Focus

In general, the IAC will leverage the considerable operational, clinical, and managerial expertise of its collaborators. It will seek out subject matter experts (SMEs) from around the world to augment that expertise, and it will disseminate uniform, consistent, and accurate homeland security and medical response information, educational material, and emergency response programs to a broader audience through the following areas of focus.

Repository of Best Information

The IAC will develop a secure electronic repository to house (1) current, relevant homeland security and medical response information and (2) policies, protocols, and programs identified by SMEs as representing best practices. The repository will include a reference database, a relational database, and a search engine component that will speed access to information within the repository and other approved databases. Information in the repository will be gleaned from an array of military, civilian, public, private, domestic, and international organizations and agencies invested in homeland security, and emergency preparedness efforts and will be evaluated by IAC staff or appropriate SMEs prior to inclusion in the repository. Secured access to current research in areas such as response to chemical, biological, radiological, nuclear, and explosive threats will provide high-quality information that will be used by IAC staff and subscribers to develop and enhance best practice policies, protocols, and programs available through the repository.

The sharing of uniform and coordinated information and best practices among military, civilian, public, private, domestic, and international homeland security partners will build national and international response capacity to address terrorist threats and other disaster events. For example, civilian response can be enhanced and federal homeland security funding can be leveraged through adaptation and incorporation of an extensive menu of emergency medical response solutions developed by the military in the areas of surge capacity, mass casualty response and recovery, education and training, and drills and exercises.

Analytical Services

The IAC will utilize expertise from the collaborators and recruited SMEs to provide information analysis services that will enhance the value of the reposi-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

tory and make it more accessible and usable to a broad audience. Services will include development and dissemination of

- a search engine available to subscribers to facilitate independent research into the repository and other approved Web content and created using specific taxonomy developed for homeland security and medical response topics
- bibliographies on selected topics
- focused technical reports, specialized white papers, handbooks, and data books that address general or specific homeland security and medical response issues
- retrospective analyses of information related to homeland security and medical responses to improve future emergency response to disaster events
- reports on existing military and civilian, public and private, domestic and international projects to minimize duplication of efforts and maximize existing investments
- identification of homeland security and medical response program gaps and engagement of groups with proven expertise to create programs to fill those gaps
- meta-analysis of repository material requested by IAC staff or by clients

IAC Technical Requirements

System Description

The IAC technical infrastructure will (1) enable staff and authorized users to initiate a secure Web connection to view and download files with a standard Web browser, (2) maintain a reference database application tied to a search engine that functions as a database of databases, and (3) maintain a relational database of documents relevant to homeland security and medical response. System components include a public Web portal, a virtual private network (VPN), a reference database, and the IAC relational database in a secured environment.

System Design

Where possible, the configuration of hardware and software will utilize existing systems and commercial off-the-shelf components. Several key components are as follows:

- Web portal and scalability: The system will utilize the single-point-of-entry concept that has been demonstrated by existing IACs; it will be designed to accommodate increasing numbers of users as utilization increases and will also facilitate redirection to existing and future database components as the system evolves.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

• Security: The system will utilize a VPN with Secure Sockets Layer pages for login and access, and a dedicated firewall attached directly to the incoming Internet connection will provide additional security; while users will include both civilian and military partners, user access will be categorized according to each user's need to know and their ability to conform to all government regulations and procedures for information security.

• Reference database: This component will store keywords and search algorithms created by subject matter, information technology, and bibliographic experts to speed acquisition and analysis of the relational database.

• Relational database: The IAC will maintain numerous relational databases, such as Microsoft SQL Server and Oracle, and requirements for the relational databases will be designed to facilitate migration to and from other existing databases.

CONCLUSION

The thought of an outbreak of disease caused by the intentional release of a pathogen or toxin in a U.S. city was alien just 10 years ago. Many people believed that biological warfare was only in the military's imagination, perhaps to be faced by soldiers on a faraway battlefield, if at all. The anthrax letters of 2001 and the resulting deaths from inhalation anthrax have changed that perception. The national, state, and local governments in the United States are preparing for what is now called *not if, but when and how extensive* biological terrorism. In contrast to the acute onset and first responder focus with a chemical attack, in a bioterrorist attack, the physician and the hospital will be at the center of the fray. Whether the attack is a hoax, a small foodborne outbreak, a lethal aerosol cloud moving silently through a city at night, or the introduction of a contagious disease, the physician who understands threat agent characteristics and diagnostic and treatment options and who thinks like an epidemiologist will have the greatest success in limiting the impact of the attack.

As individual health care providers, we must add the exotic agents to our diagnostic differentials. Hospital administrators must consider augmenting diagnostic capabilities and surveillance programs and even making infrastructure modifications in preparation for the treatment of victims of bioterrorism.

Above all, we must educate ourselves. If we respond correctly, preparation for a biological attack will be as dual use as the facility that produced the weapon. A sound public health infrastructure, which includes all of us and our resources, will serve this nation well for control of the disease, no matter what the cause of the disease.

Copyright National Academy of Sciences. All rights reserved.

On the Events in Beslan

Gennady Kovalenko
Presidium of the Russian Academy of Sciences

The causes, course, and consequences of the terrorist act in Beslan are being discussed both within Russia and beyond its borders. Analysts in the media are expressing the most varied and at times directly contradictory judgments, lessons, and conclusions on what happened. Today it would be premature to issue final assessments of the events in Beslan without waiting for the results of the work of the parliamentary commission investigating the causes and circumstances of the terrorist act in North Ossetia or the conclusion of the investigation on the criminal case that has been opened by the General Prosecutor's Office. Therefore, these tragic events may be analyzed and certain conclusions drawn only in preliminary fashion.

THE OPERATIONAL SITUATION PRIOR TO THE TRAGEDY IN BESLAN

The events in Beslan bring to mind the seizure of hostages at the theater in Moscow in October 2002 (during a performance of *Nord-Ost*). These two major terrorist acts have a certain similarity: They involved the taking of massive numbers of hostages, numerous fatalities, and destruction of the terrorists. Those who carried out the terrorist acts in both cases put forth intentionally unacceptable demands for the withdrawal of federal forces from Chechnya in an attempt to compel the Russian leadership to enter into talks with the leaders of the Chechen militants. Both terrorist acts shook all of Russian society and once again drew world public attention to the actions of the Chechen fighters. It is no accident that a Chechen Web site called the terrorist act in Beslan *Nord-Vest*.

The *Nord-Ost* seizure marked a change in the tactics of the Chechen terror-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

ists. In fact, it was the first major terrorist act carried out by members of the so-called Riyadus Salihiin scouting and sabotage battalion created by Shamil Basaev (in Arabic, "Riyadh as-Salihiin" means "gardens of the righteous"). Among the activities of this group was the training of suicide fighters. The battalion was assigned the task of waging mine warfare and carrying out acts of sabotage in Chechnya and other Russian regions involving suicide bombers. Approximately 150 young men and young women were selected for the battalion and consecrated as so-called suicide fighters.

In creating such an important-sounding group, Basaev was pursuing another goal, namely raising the status of the Chechen terrorists and consequently increasing their funding from abroad. They would be part of the international terrorist network and would assume their honorable place among similar world-famous organizations. Basaev even changed his name to the Arabic style—Abdullah Shamil Abu Idris.

The majority of the most significant terrorist acts in 2003 were carried out by suicide bombers, or shahids. One of the main goals of the terrorist acts was to destroy the process of normalization of the North Caucasus situation and to have a negative impact on the population of primarily this region before the State Duma elections.

In 2004 we saw a sharp increase in terrorism, culminating in the events in Beslan. It was the year of the Russian presidential election, so the results of Vladimir Putin's first term as president were being summed up. The Chechen presidential election was also held in 2004, the very fact of which was supposed to consolidate the republic's turn toward peaceful life. This was also the year of the sixtieth anniversary of the deportation of the peoples of the Caucasus, and the Chechen fighters marked such important dates with bloody acts.

However, there are also other reasons for the increased activities of the terrorists. The numerous terrorist acts, sabotage, murders, and abductions they carried out in 1998–2004 did not lead to any politically significant results. This could not but evoke serious complaints against the leaders of the bandit groups on the part of the foreign sponsors financing their activities. To prove their professional suitability, Basaev and Aslan Maskhadov had to carry out a series of particularly major terrorist acts.

In Moscow on February 6, 2004, there was a powerful explosion on a subway train car between the Paveletskaya and Avtozavodskaya stations, in which 39 people were killed and about 350 passengers were wounded, of whom 122 were hospitalized. According to the initial findings of the investigation, the terrorist act was carried out by a suicide bomber.

On May 9, 2004, during a holiday concert at Dynamo Stadium in Grozny, an explosive device was detonated. It was later learned that the device had been placed during construction and repair work at the stadium. Seven people were killed in this terrorist act, including Chechen President Akhmad Kadyrov and Chechen State Council Chairman Khusein Isaev. Colonel-General Valery

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Baranov, commander of the joint group of forces in the North Caucasus, was seriously wounded, and 73 others were also injured. Basaev soon claimed responsibility for the terrorist act.

In June through August of 2004, an unprecedented series of terrorist acts posed an urgent question for the Russian authorities regarding the need to intensify the total struggle against terrorism.

The terror escalation began with an armed raid by Chechen bandit formations into Ingushetia. On the night of June 21–22, more than 300 fighters under the command of Shamil Basaev took control of Nazran and Karabulak for several hours. They simultaneously attacked the local headquarters of the Federal Security Service, the special purpose police brigades (OMON), and interior ministry troops and practically destroyed the Nazran Region police station. They seized equipment from the supply facility of the Ministry of Internal Affairs in Karabulak, which held hundreds of weapons and tens of kilograms of explosives. After setting up checkpoints on the roads, the fighters searched passing vehicles and shot on sight all members of law enforcement and the military. On the morning of June 22, after loading more than 600 weapons and explosives into their vehicles, the fighters headed toward the Chechen border. During the raid, more than 100 people were killed, including senior officials from the local Ministry of Internal Affairs and the Ingushetian public prosecutor's office. The action in Nazran revealed substantial shortcomings in the regional government system and a lack of effective coordination among local law enforcement agencies and the federal forces deployed in the Caucasus. A subsequent investigation uncovered instances in which the bandits were aided by several members of the Ingushetian police force.

As later events showed, the attack on the Ingushetian cities was a sort of scouting mission, a preparatory stage in a preplanned series of bloody terrorist acts, the number of victims from which would be comparable with U.S. losses on September 11, 2001.

On August 21, the fighters carried out a bold operation against federal forces in Grozny. About 300 armed bandits set up checkpoints on the roads and for three hours attacked police stations in various districts of the city and fired on polling stations. When darkness fell, the fighters left. According to information from local government officials in the Oktyabrsky and Staropromyslovsky districts of the Chechen capital, combined fatalities among federal troops, the police, and the local population totaled 78. At least 25 fighters were killed during the operation, and some of those killed were carried away by the bandits. It has been established that the raid on Grozny was led by Brigadier General Doku Umarov, who had been one of the organizers of the recent attack on Ingushetia.

In Moscow on August 24, a bombing at a bus stop on Kashirskoe Shosse left four people injured. It was only due to luck that no one was killed in the incident. A terrorist attack on the night of August 24–25 caused two Russian airliners that had departed from Moscow's Domodedovo Airport to crash only a few minutes

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

apart. A total of 90 people were killed, including all the passengers and crew. According to materials gathered during the investigation, the planes were blown up by two Chechen suicide terrorists, who together with two other Chechens arrived at Domodedovo on August 24 on a flight from Makhachkala. The investigation established that the terrorist acts were facilitated to a significant extent by shortcomings in the flight security system. Cases of corruption on the part of individual airport employees were also uncovered.

Not long after, on the evening of August 31, a female terrorist suicide bomber carried out the next act of terror near Moscow's Rizhskaya Metro Station, in which 10 people were killed and about 50 wounded. The yield of the explosive device was equivalent to 1.5–2.0 kilograms of TNT.

The plane crash incidents led to the first international investigation. An announcement appeared on a little-known Arabic Web site that a certain Islamist group, the Islambullah Brigades, had claimed responsibility for bombing both planes. However, a preliminary investigation showed that the terrorist acts in Moscow and on both planes were planned and carried out by members of the so-called Karachai *jamaat*, Muslim Society Number 3. The group is headed by terrorist Achimez Gochiyaev, wanted in regard to the Moscow apartment building bombings of 1999 and currently in hiding in the Republic of Georgia. A cellular phone found on the terrorist killed at the Rizhskaya Metro Station continued receiving calls from the Georgian Pankisi Gorge even after her death. The culmination of the massive attacks by terrorists came with the events of September 1–3, 2004, in North Ossetia.

THE COURSE OF EVENTS IN THE BESLAN TRAGEDY

How did events develop in Beslan? On September 1, 2004, a group of terrorists seized Beslan's School Number 1, taking more than 1,200 hostages, including students, their parents and relatives, and teachers. Unfortunately the law enforcement agencies and units of other related structures had no warning that this terrorist act was being planned.

The organizer of this terrorist act was Shamil Basaev. His Ingushetian colleague Magomet Yevloev led the group of fighters, and the action was financed by al Qaeda's representative in Chechnya, Abu Omar. According to available information, Aslan Maskhadov participated directly in planning the operation. Many fighters who took part in the school seizure did not know one another and were told of the plan for the terrorist act just before they left for Beslan. The hostages got the feeling that the terrorists were blindly carrying out someone's plan to seize the school but did not know what to do after that. According to information that has been received, the bandits spoke several times by telephone with unknown parties in Middle Eastern countries, particularly the United Arab Emirates.

It has been established that the group of terrorists entered the city in two

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

vehicles traveling from the direction of the village of Khurikau, Mozdok Region, in the Republic of North Ossetia-Alania, which is 30 kilometers from the administrative border with Ingushetia. The terrorists brought all of their weapons, equipment, and explosive devices with them. The story that weapons had supposedly been hidden in the school in advance during renovation work over the summer has not yet been confirmed.

After receiving an alarm that hostages had been seized, local police personnel blocked off access to the school. Additional police forces, units from the Russian Interior Ministry troops and armed forces, and emergency medical personnel subsequently arrived on the scene. Units from the Special Purpose Center of the Russian Federal Security Service were immediately sent to Beslan from Khankala, Yessentuki, and Moscow. An operational headquarters under the command of North Ossetian President Aleksandr Dzasokhov was established by order of the government of the Russian Federation to directly manage the counterterrorist operation.

After beginning its work, the operational headquarters issued orders to strengthen the first and second blockade perimeters around the area of the school and to evacuate residents of nearby homes. The operations zone was cordoned off by units from the armed forces and interior troops from the Russian Ministry of Internal Affairs and forces from the Ministry of Internal Affairs of North Ossetia.

In the cordoned-off area and surrounding zone, targeted work was carried out to find accomplices of the terrorists. The necessary measures were taken to determine the exact number of hostages. To this end, the local authorities conducted the necessary surveys of relatives, neighbors, and other persons who might provide such information.

An evaluation of the situation on site indicated its extreme complexity. The hostages had been divided into groups and placed in various parts of the school. A large number of people were gathered in the gymnasium. Groups of 100 or more hostages were located in other school buildings. All of the locations where the children and adults were being held had been mined by the terrorists. From an analysis of information on the system by which the mines had been laid at the school, authorities concluded that it would be practically impossible to disarm the devices because they were equipped with a dual-control system. Furthermore, if the terrorists lost control over the mine system, the detonation command would be given not intentionally but automatically. The death of the terrorists who were keeping the device control chain open would inevitably lead to the detonation of all the explosive devices. The terrorists had constructed the system so as to kill the maximum number of hostages and special forces personnel if they attempted to undertake any actions by force. The terrorists used 14 homemade shrapnel bombs and 4 antipersonnel bounding fragmentation mines. They had in their possession 8 reactive grenade launchers, 6 Shmel (Bumblebee) infantry flamethrowers, and 17 hand grenades.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

It has been established that a significant number of the terrorists were under the influence of narcotics, and their actions were difficult to predict. According to available information, they had used so-called military narcotics, which later allowed even several wounded fighters to continue active armed resistance.

The criminals limited all contacts with the outside world and for a long time avoided negotiations. They did not use any means of communications so as not to give the relevant security services an opportunity to intercept their transmissions. It was rather difficult to obtain information on the situation inside the school or the actions of the terrorists.

Immediately after the seizure of the school, the terrorists began shooting some of the hostages and at times engaged in random gunfire, in this way trying to provoke the special forces units into taking forcible action. In all, 21 people were killed in the first day of the terrorist act. Information coming into the operational headquarters attested to the extremely difficult situation for the hostages, who were being denied food and water.

Taking this into account, the operational headquarters considered various scenarios by which events might develop. They did not rule out the possibility of the mass annihilation of the hostages by the terrorists, who might subsequently attempt to escape. If this were to happen, a special plan of actions by the special forces was created. However, because of the way the situation developed over time, operational headquarters realized that it would be impossible to avoid massive casualties among the hostages if the plan were to be carried out.

Proceeding on this basis, the operational headquarters focused its primary efforts on negotiating with the terrorists with the aim of freeing and saving the maximum possible number of people. In the initial phase of the negotiations, the headquarters called in the mufti of the Spiritual Board of Muslims of North Ossetia, but the terrorists refused to speak with him or with other muftis invited from Ingushetia and Chechnya. The attempts of the well-known pediatrician Leonid Roshal to establish stable contact with the terrorists also failed. Also involved in the negotiations were former Ingushetian President Ruslan Aushev and well-known entrepreneur Mikhail Gutseriev. The participation of these individuals brought about somewhat more active contacts with the terrorists. As a result of negotiations involving Ruslan Aushev, the terrorists freed 26 hostages (13 children under two years of age and their mothers) on September 2.

Meanwhile, measures were being taken to determine the identities of the terrorists and locate their relatives and close connections for use in the negotiation process. Thus the wife and three children of Iznaur Kodzoev, one of the terrorists, were brought to Beslan. Kodzoev's wife recorded a video appeal to the terrorists asking them to free the children being held hostage. Kodzoev categorically refused and declared his intention to kill any relatives who might attempt to negotiate with him.

The operational headquarters also considered the possibility of exchanging the hostages for detained participants in the armed attack on Ingushetia in June

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

2004 or of paying the terrorists a monetary ransom and providing them with transportation and the opportunity to escape unimpeded into Chechnya.

It should be noted that the terrorists were not eager to participate in the negotiations and made practically no demands. Through Aushev they passed along intentionally unacceptable demands supposedly on behalf of Basaev, namely to "grant sovereignty to Chechnya and remove federal troops from it." The terrorists named Maskhadov as a possible interlocutor in the negotiations. The operational headquarters attempted to communicate with him; however, Maskhadov did not make contact.

The addition of Russian presidential aide Aslambek Aslakhanov to the negotiation process gave rise to certain hopes for its positive continuation. After noon on September 3, an agreement was reached with the terrorists on the removal from the school building of the bodies of the hostages killed, and a group of four individuals from the Russian Ministry of Emergency Situations approached the school in a truck. At that moment, two explosions occurred in the gymnasium where some of the hostages were being held. The gymnasium was partially destroyed and a fire broke out. The exact cause of the explosions has yet to be established. According to information from several hostages, the terrorists were in a state of drug intoxication, and that may be why they lost control of the explosive devices, which were automatically detonated. In the panic that broke out after the explosions, some of the hostages made their way out of the school building and attempted to run. The terrorists opened deadly fire on the fleeing women and children.

In this situation the headquarters ordered troops from the Special Purpose Center of the Russian Federal Security Service to advance on the school in order to evacuate the hostages and eliminate the terrorists' firing positions. The approach to the building was made under heavy fire from the militants. The process of advancing to initial positions and suppressing the terrorists' firing positions was complicated by the actions of local residents armed with guns, who had broken through the cordon and randomly opened fire in the direction of the school.

Freeing the hostages and destroying the terrorists took more than 10 hours. This was associated with the presence of a large number of wounded hostages in the school. Personnel from the Special Purpose Center had to render them urgent assistance and evacuate them from the school. Defending themselves, the terrorists dispersed and, using children and other hostages as human shields, waged an intense armed resistance. During the battle, personnel from the Special Purpose Center devoted greater attention to saving the hostages than to destroying the terrorists. Thus the special units suffered heavy losses: 10 of their personnel were killed and 41 suffered wounds and contusions.

A total of 330 people were killed in the terrorist act in Beslan, including 186 children (172 according to other information), and more than 700 people were seriously wounded. All of the bodies of those killed have been identified, of

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

whom 81 (including 54 children) were identified as a result of molecular genetic analysis.

A total of 31 terrorists were killed during the military clash, and 17 of them have been identified. According to a statement from the operational headquarters, none of the terrorists managed to hide. One of them was arrested. He was Nur-Pasha Kulaev, a native of the village of Seyasan, Nozhai-Yurt Region, in the Chechen Republic.

Information published in several media outlets (particularly in the newspaper *Komsomolskaya Pravda*) purporting that 52 fighters participated in the school seizure and that one female suicide bomber was taken alive have turned out to be incorrect. The newspaper later printed an appropriate retraction.

According to information from the office of the general prosecutor for the North Caucasus, an Ingushetian resident has been arrested under suspicion of aiding the terrorists during preparations for the attack on the population centers in the Republic of Ingushetia on June 21–22, 2004, and for the terrorist act in Beslan.

During the operational investigation on the criminal case filed by the Russian General Prosecutor's Office regarding the school seizure and murders of the hostages, it has been established that Basaev directly planned the attack. According to preliminary information, some of the terrorists were members of the terrorist group Riyadus-Salihiin. The group included individuals from Chechnya and Ingushetia and mercenaries from Arab countries. The investigation has now managed to determine the identities of 17 of the terrorists killed, including their leader, Ruslan Khuchbarov, a native of the village of Galashki in the Chechen-Ingush Autonomous Soviet Socialist Republic, and an Ingushetian by nationality. From the investigation of this criminal case, five local police officers have also been accused of negligence. According to a recent report from a representative of the General Prosecutor's Office, six individuals suspected of aiding the terrorists have been arrested.

CONCLUSIONS

The events in Beslan, the armed terrorist attacks against Ingushetia and Grozny in the summer of 2004, and the terrorist acts in Moscow are all part of the unified strategy of the ideologues of international terrorism, namely to expand their influence as widely as possible, create an atmosphere of universal fear, cause the population to distrust the capabilities of the government, and to force its leaders to enter into negotiations with the leaders of the bandit formations.

The situation in the North Caucasus remains rather complex, as shown by 2004's series of terrorist acts. The leaders of the Chechen fighters are making focused efforts to spread instability not only to Chechnya but also to the majority of adjoining territories.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Chechen bandit formations, which by various accounts number 2,000 to 3,000 members, of whom about 200 are foreigners, have lost the capacity to wage wide-scale military operations, but they continue their bandit tactics of inflicting appreciable blows on the federal forces and local law enforcement agencies, actions that also produce casualties among the civilian population. Bombings of transportation facilities and vehicles continue, along with shootings of military and law enforcement personnel. Active use is being made of the infrastructure the terrorists have created—bases; caches of weapons, hardware, and ammunition; and accomplices among the local population.

It should be noted that this is not the first time that North Ossetia has been the target of terrorist attacks. More than 10 terrorist acts have been carried out here in the past five years. The most severe among them were the bombing of the central market in the city of Vladikavkaz (March 1999, 53 people killed and 168 wounded), the bus explosion carried out by a female suicide bomber (June 2003, 19 victims), the bombing of the Mozdok Hospital (August 2003, 50 killed), and others.

This is no accident. The republic has a key position in the North Caucasus. With its majority Orthodox population, North Ossetia has experienced practically no internal interethnic problems in recent years. Tensions have remained on the border with Ingushetia, along with the conflict in Tskhinvali. In this regard, one of the goals of the terrorist act in Beslan was to cause new clashes between Ossetians and Ingushetians and open a sort of second front in the North Caucasus.

The events of 2004 showed that Chechen fighters have a certain base of accomplices in the region. Assistance provided to the terrorists by individual local residents is an acute problem that seriously complicates the struggle against the bandit formations. One reason for this negative phenomenon lies in the firm familial and clan ties that link entire villages and regions. However, the fundamental factor destabilizing the situation is the extremely low standard of living of the local population. Payments for aiding the fighters often represent a person's only source of income.

As the Russian leadership has acknowledged, the economic picture in the North Caucasus region remains pitiful, and therefore it is simultaneously a victim of the bloody terror and a platform for its replication. The roots of terrorism lie in massive unemployment and the lack of an effective social policy.

In particular, graphic evidence of this may be found in many statistical indictors on the Southern Federal District, which are significantly lower than both Russian averages and development indicators for other federal districts. For instance, the gross regional product per capita is only 53 percent of the Russian average and from 30 to 71 percent of the same figure for other federal districts. Rates of increase for basic capital investments also lag significantly behind statistical averages. Moreover, the Southern Federal District has practically the highest proportion of completely worn out or obsolete fixed assets, especially in

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

such industries as agriculture, construction, and transportation. Further evidence of the region's economic crisis may be found in the fact that average per capita income is 34.5 percent lower than for Russia on the whole, while the average monthly salary is 69 percent of the Russian level and 50 to 71 percent of the level in other federal districts. The unemployment rate in the Southern Federal District is two to five times higher than in other districts (the number of unemployed comprises 35 percent of the total number of unemployed in the entire country). In Ingushetia, 72 percent of the able-bodied population is unemployed (according to an interview with Ingushetian President Murat Zyazikov). All of this ultimately creates the preconditions for social dissatisfaction and mistrust of the authorities and reduces the effectiveness of antiterrorist measures, something in which the leaders of the bandit formations have a great interest. The local authorities undoubtedly bear a significant share of responsibility for the serious socioeconomic situation in the region. The events in Beslan and the results of the earlier armed raids on Nazran and Grozny revealed significant shortcomings in the regional administrative system along with departmental disconnections and a lack of effective coordination among local law enforcement agencies and the federal forces deployed in the Caucasus.

Although the results of the work of the parliamentary commission investigating the terrorist act in Beslan will be presented no earlier than March 2005, the commission's leaders have already announced several preliminary conclusions that have been published in Russian media outlets. For instance, in the opinion of the commission's chair, Vice Speaker of the Federation Council Aleksandr Torshin, one of the main causes of the tragic events in North Ossetia was the irresponsibility of local bureaucrats at various levels, who were incapable of making independent decisions and could only await instructions from Moscow. The commission had serious complaints regarding the law enforcement agencies, who were unable to coordinate their activities in this emergency situation. They found themselves unprepared for the scenario by which events developed in Beslan, and the operation to free the school occurred in spontaneous fashion, particularly in its initial stage. Many serious mistakes were made.

The commission uncovered cases of corruption in the work of the republic's law enforcement agencies. Four participants in the terrorist act in Beslan had previously been detained by the local police but were later released without justification. One of these four bandits, Mairbek Shabikhanov, was arrested as a participant in an attack on a federal troop column that involved numerous casualties. He was accused under three articles: banditry, illegal possession of a weapon, and murder. However, on July 7, 2004, he was acquitted on all counts by a jury in the Republic of Ingushetia. Almost immediately after he was freed, Shabikhanov and his suicide bomber wife set off for Beslan. The reason behind such a strange verdict was found in familial ties, which permeate all local agencies, including the law enforcement system. Clear oversights were discovered in the work of the law enforcement agencies of Ingushetia, which should have

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

known about the existence in their republic of a training camp for the fighters who later seized the school in Beslan.

In the commission's opinion, the lack of the appropriate reaction by the authorities to the previously committed terrorist acts had a very harmful influence on the development of the situation in the region. No one took personal responsibility for the attempted assassination of Ingushetia's leader Murat Zyazikov in March 2004, the murder of Akhmad Kadyrov in May, or the attack on Nazran on June 21. Only the actions of the special forces personnel merited a positive evaluation from the commission, although certain criticisms were also addressed to their leaders, who did not manage to consider all possible options for the development of the situation.

The events of last year show that despite the terrorist acts, which involved significant casualties, the struggle against the terrorist network in the North Caucasus is gradually achieving its goals, although far more slowly than we would like. The terrorists have not managed to achieve the goals they set for themselves. The terrorist act in Beslan did not lead to the outbreak of an Ossetian-Ingushetian conflict. The Chechen terrorists are already incapable of engaging in wide-scale military conflict with the federal forces and are increasingly targeting facilities in the educational and sociocultural spheres and the transportation infrastructure, where minimal efforts and expenditures will lead to maximum results—numerous casualties among the civilian population.

It must be noted that the terror escalation in 2004 was accompanied by the rise of ideological extremism. Ingushetia, Dagestan, and Karachaevo-Cherkessia saw increased activities on the part of Wahhabist *jamaats*, which serve as suppliers of new fighters for illegal armed formations. In a number of regions of the country, law enforcement agencies have discovered cells of the well-known extremist organization Hizb ut-Tahrir al-Islami.

The expanded export of radical ideologies to Russian territory has been noted recently (analogous processes are also occurring in other countries of the Commonwealth of Independent States). Extremist organizations (mainly carriers of the ideas of radical Islam) are making persistent efforts to spread ideas of an openly subversive nature among the population, especially among the youth.

Against this backdrop, one may see a clear ideological passivity on the part of both state and public institutions with regard to using information to counter the spread of extremist ideas, especially radical Islam. The destructive influence of these ideas on certain segments of the population that have been unable to find a place for themselves in new socioeconomic conditions has been clearly underestimated.

Financial support from various international terrorist and extremist organizations is another no less significant source for the activism of the organizers and executors of acts of terrorism and sabotage. The terrorist acts of last year showed that for the majority of terrorists, committing these bloody crimes is only business.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

In 2004, law enforcement agencies obtained the latest specific materials on the financing of the activities of Chechen fighters by foreign sponsors. For instance, the Arab mercenary Abu al-Walid, the main distributor of funds sent to Chechnya by various foreign organizations (subsequently liquidated by federal forces) received $4.5 million in February 2004 for the Moscow metro attack alone.

A foreign mercenary arrested in Dagestan in 2004 who, as later became clear, had ties with certain foreign government agencies, confirmed in the course of interrogation the existence of close business contacts between the leaders of the Chechen bandit formations and al Qaeda, as well as al Qaeda financing of terrorist activities in the North Caucasus.

In early 2005 the personal archives of the terrorist Abu Kuteiba were discovered in Chechnya. Abu Kuteiba, who is of Arabic origin, was involved in financing terrorist activities in Russia from abroad. With the help of the financial documentation that was seized, it was possible to trace the path by which money was sent to carry out terrorist acts, including through the purchase of weapons, payments to fighters for specific terrorist acts, payments of transportation expenses, and so forth.

MEASURES TAKEN IN CONNECTION WITH THE EVENTS IN BESLAN

The tragedy in Beslan required federal government agencies to undertake a wide range of administrative, legislative, economic, and other measures.

On September 13, 2004, the president of the Russian Federation issued Decree No. 1167 on Urgent Measures to Improve the Effectiveness of the Struggle against Terrorism. Under this decree the Russian government, the Ministry of Defense, and law enforcement agencies were assigned the task of developing a set of measures to improve state policy for ensuring the security of the Russian Federation and intensifying the struggle against terrorism.

Administrative Measures

Soon after the Beslan tragedy, Dmitry Kozak was appointed plenipotentiary representative of the Russian president to the Southern Federal District and given additional authorities. Meanwhile, the Russian Federation Ministry of Regional Development was created by presidential decree, and former plenipotentiary representative to the Southern Federal District Vladimir Yakovlev was named as its head.

The Commission on the Coordination of the Activities of Federal Executive Branch Agencies in the Southern Federal District was established on orders from the president. As a component of the overall crisis management system developed by the presidential administration, the commission was created to prevent

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

and suppress terrorist acts and to detect and eliminate the causes and conditions that allow them to be planned and carried out. From analysis of the situation in the North Caucasus, the country's political leadership concluded that the system for civilian, military, and law enforcement management in the region was insufficient to meet the terrorist challenges and therefore undertook a radical restructuring of that system. Operational antiterrorism management groups have been created under the auspices of the antiterrorist commissions in all regions of the Southern Federal District. These groups are headed by 12 officers from the interior troops of the Ministry of Internal Affairs, who have been accorded the status of deputy chairs of the above-mentioned commissions. They have been assigned the task of coordinating the efforts of all military and law enforcement structures represented in the members of the Russian Federation to counter the terrorist threat. In accordance with Decree No. 1167, the government, in cooperation with military and law enforcement agencies, has prepared recommendations on improving the system for coordination of forces and resources involved in resolving the situation in the North Caucasus.

Legislative Measures

The State Duma has created a Commission on the Problems of the North Caucasus, and its scope of responsibilities will primarily include the region's socioeconomic problems. A joint commission of the Federation Council and the State Duma has also been established to study the terrorist act in Beslan, and it is headed by Federation Council Deputy Chair Aleksandr Torshin.

In cooperation with the government, the legislators must review and ratify a package of measures developed to combat terrorism, which impact more than 40 existing laws. Their first tasks include creating a unified legal base for the struggle against terrorism, radically changing the ways in which all the intelligence services interact, and expanding their powers.

In particular, the package of bills includes a change in the Law on Combating Terrorism. The events in Beslan showed that the vagueness of certain provisions in the existing law has a negative impact on the effectiveness of operations to render terrorists harmless. The law does not clearly stipulate who should be responsible for leadership of the military and law enforcement structures in situations like the Beslan attack. One of the goals of the law is to give the authorities and the law enforcement and military structures a legal base that will make it possible to minimize losses of not only time but also results. This draft federal law strengthens the legal foundations for countering terrorism, including not only the grounds, conditions, and procedures for carrying out measures to combat terrorism but also a range of measures of a political, socioeconomic, informational-promotional, organizational, and legal nature related to counterterrorism activities in general. One of the conceptual provisions of this bill is that it is significantly focused on the prevention of terrorism in all its forms and

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

manifestations, with the understanding that this activity will involve practically all government agencies, which is one of the principal aspects by which it differs from the existing law.

An important new feature in the bill is its introduction of the concept of terrorist danger. It defines terrorist danger and the conditions and procedures for instituting a terrorist danger regime, and measures that can be taken in the zone in which such a regime is in effect.

Another aspect of a conceptual nature is that the bill proposes a solution for a long-standing problem with the legality of the participation of the armed forces of the Russian Federation in counterterrorist operations. The bill establishes the legal foundations for their participation in such operations, and it defines the right to use weapons and military hardware in cases spelled out in the bill.

The bill sets forth a clearly constructed system for managing counterterrorism efforts. Under ordinary circumstances, leadership and coordination of the activities of all entities involved in countering terrorism are the responsibility of the antiterrorist commissions, but from the moment a terrorist danger regime is instituted or a decision is made to conduct counterterrorist operations, leadership of all forces and resources of all counterterrorist entities is assigned to agencies of the Federal Security Service.

Passage of the new Law on Countering Terrorism will undoubtedly help to make the struggle against terrorism more effective and to ensure the security of the Russian Federation.

Measures of an Economic Nature

The State Duma Commission on the Problems of the North Caucasus intends to create a Concept for the Development of the North Caucasus, which will include a comprehensive program of measures regarding the region's economy. It will also call for the development of the transportation network, the Caspian ports, and hydroelectric power facilities; the strengthening of traditional agricultural sectors (viticulture, sheep raising, and so forth); the creation of new jobs by establishing assembly plants for enterprises in the Russian military-industrial complex; the expansion of the infrastructure for ecotourism in certain North Caucasus regions; and so on. The program will include recommendations on restructuring the debts of local enterprises and establishing preferential tax benefits for investment projects.

The Russian government has prepared a program outlining specific measures to be carried out to rehabilitate the situation in Beslan, specifically including the construction of schools, hospitals, and other elements of the urban infrastructure. The president has assigned the government the task of developing a well-considered and effective policy for the Federal Center on the North Caucasus to resolve the region's most urgent socioeconomic problems quickly.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

In the Sphere of International Cooperation

International terrorism has become a factor that is seriously destabilizing individual countries and regions and the world as a whole. Naturally the struggle against this evil can produce results only if effective international cooperation is established. In connection with last year's terror escalation, the Russian leadership has proposed a further intensification of international cooperation in the struggle against the terrorist threat. At the fifty-ninth session of the United Nations General Assembly, Russian Foreign Affairs Minister Sergei Lavrov announced a plan for combating the "global terrorist international," which included a condemnation of countries that provide asylum to terrorists and their accomplices and sponsors. In the opinion of the Russian leadership, the struggle against terrorism must include the active participation of the main international organizations—the United Nations, the governing structure of the G-8, the Russia-NATO Council, the Organization for Security and Cooperation in Europe, the Council of Europe, the Financial Action Task Force on Money Laundering, and others.

Within the context of international cooperation, I would like to mention the obvious relations of certain official representatives of Western countries with Chechen terrorists, who they often call rebels. After the latest major terrorist act in Russia, numerous condolences were received from abroad, the sincerity of which is difficult to doubt. However, last year the "minister of foreign affairs" of the underground government of so-called Ichkeria, Ilyas Akhmadov, received political asylum in the United States; "Vice Premier" and "Minister of Culture" Akhmed Zakaev lives quietly in England; "Minister of Health" Umar Khanbiev has been given shelter in France; and the "minister of social issues" receives a stipend from the Heinrich Böll Foundation in Germany.

Of course, such differences in approach cannot seriously impede the fruitful process of struggle against this common evil. One example is today's meeting. The need for further cooperation between Russia and the United States in countering the new terrorist threat is completely objective in nature. In particular, the closest cooperation is essential in such areas as improving the base of international laws on the struggle against terrorism and mechanisms for rendering mutual legal assistance (including the mutual extradition of terrorists and furtherance of the principle of certain punishment), closing down channels for the financing of terrorism, preventing weapons of mass destruction and means for their delivery from falling into the hands of terrorist groups, and strengthening controls over the trade in conventional weapons and explosives. To promote coordinated bilateral and multilateral actions, judging by the statements of Russian officials, Russia is prepared to move forward to the point of expanding operational exchanges of information and even conducting joint counterterrorist operations.

As has been noted, including by U.S. experts, creation of a broad coalition is

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

fundamentally important for success in the struggle against terrorism. Terrorism has now become one of the main threats to the security of the Russian Federation. In order to improve the effectiveness of counterterrorist activities, we must make a timely analysis of the experience amassed by other countries, specifically the United States, in the struggle against terrorism. In this regard, the recommendations on countering terrorism developed by the National Commission on Terrorist Attacks Upon the United States (the 9-11 Commission) may be of practical interest. They are outlined in the final report published by the commission in July 2004 on the results of its almost two years of work. The urgent need to analyze the recommendations and conclusions of this national counterterrorist commission and the forms of organization of its work are heightened in connection with the activities of the Russian Commission of Representatives of Both Chambers of the Federal Assembly of the Russian Federation on Investigating the Terrorist Act in Beslan.

The nature of the debates regarding preliminary information on the commission's work indicates that answers along the lines of "Who is to blame?" or "Why did such a thing become possible?" are less pressing for the public than answers to the questions "What must be changed?" and "How can we prevent it?" We hope that the conclusions and recommendations will promote a successful resolution of the specific issues facing Russia.

Copyright National Academy of Sciences. All rights reserved.

Measuring Progress, or Lack Thereof, in Combating Terrorism

Raphael Perl
Congressional Research Service

There is an old saying: Throw your darts and where they land, that is the target. There is a tendency of governments engaged in a particular strategy to want to justify success of the strategy. We need to measure success using broad-based objective criteria, and not criteria solely applicable to existing policies.

Among the various government agencies involved in antiterrorism efforts there is currently no common definition of terrorism and no common set of criteria for measuring success. Many agencies are still attempting to establish and define their criteria, without which they cannot measure organizational performance.

How we perceive and measure progress is central to how we formulate and implement antiterrorism strategy. It has a major impact as well on how we prioritize and allocate resources. As we cannot eliminate terror, and risk is everywhere, our perceptions of progress drive our allocation of finite resources. On the other hand, the parameters we use to measure progress set the framework for measurement of our failures. To better define the parameters of success, it is important to determine what both terrorists, and those who fight terror, see as their goals and priorities.

Understanding failures is central to success in combating terrorism. If we terminate two-thirds of the senior leadership of a particular terrorist organization, the ranks of the organization may grow and decentralize, similar to what happens when we attack drug cartels. To what degree should this be regarded as a failure rather than a success? Also, how do we measure the impact of unintended consequences—or side effects and by-products of our actions, for example, loss of civil liberties?

Progress may be defined differently by the terrorists and those who oppose

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

them. Hence both can claim progress and both can be correct in their assessments. How does one deal with or reconcile this?

In designing metrics, we might begin with three major categories: incidents, attitudes, and trends.

1. **Incidents**—We see reports of incidents in publications such as the Department of State's *Patterns of Global Terrorism*.[1] How widespread are incidents geographically; how deadly are they? We should also be concerned about the psychological and social impact of incidents, the economic and social costs of our response to them, and their negative effects on the macroeconomy.

2. **Attitudes**—They drive both terrorism and the world's response to terrorism. How do attitudes affect political decisions and sentiments in countries to contain and defeat terrorism, or to support it? How long can democratic governments pursue policies that pressure terrorists if such policies are seen as stimulating terrorist retaliation? Similarly, how much increase in economic costs and reduction in civil liberties will public opinion tolerate? Shaping attitudes to break or weaken the political will to combat terrorism is a central terrorist goal and an important indicator of their, and our, success or failure.

3. **Trends**—Measurement of trends is particularly relevant to terrorist infrastructure. Are we weakening their leadership; is their recruitment base, or network, growing? Relevant also are intentions (tactical and strategic goals). Have the intentions of a movement or group changed, and if so, are they more or less radical—more or less focused on causing widespread damage? Capabilities are important as well. What are the capabilities of a terrorist group to inflict serious damage? Are they increasing or decreasing?

In our search for meaningful criteria, the academic, engineering, and scientific community has much to offer government policy makers. A useful start might be simply to conduct a survey of what data on terrorism—especially databases—exist, what categories and details are found within that data, and to which topics the data are particularly relevant. Methodologies for measuring progress in combating complex social phenomena such as drug trafficking and crime may have much to offer as well. We might wish to see the results of statistically sound attitude surveys in various countries, repeated periodically. Moreover, if the academic and scientific research community is not satisfied that the government is providing a comprehensive and rigorous accounting of the bottom line in the campaign against terrorism, what prevents an organization like the National Research Council from issuing an annual report card to the nation?

The global campaign on terror is costly. It is costly in dollars spent, lost opportunities, and human lives lost or damaged. It is costly in political capital

[1]U.S. Department of State. 2004. Patterns of Global Terrorism. Washington, D.C.: U.S. Department of State.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

with our allies, in the image of the United States abroad, and in civil liberties worldwide. Some argue that the biggest threat to democracy from terrorism is not rapid destruction of property and life, but rather slow erosion of civil liberties. In addition, others argue that we are overreacting, and that we are bleeding ourselves dry economically—like the Soviet Union did in its attempts to match our military spending during the cold war. Terrorism is a nonlinear and asymmetric phenomenon. Moreover, some terrorist operations are relatively inexpensive to organize and carry out, especially compared with the damage they may inflict. Consequently we cannot expect that by spending more money we will necessarily increase our security proportionally.

According to the Government Accountability Office (GAO), the federal government currently spends $50 billion a year on homeland security. The U.S. Department of Defense has received $201 billion since September 11, 2001, for combat-related expenses in Iraq and Afghanistan and for enhancing security at military installations. During the next decade, military operations in Iraq and Afghanistan alone could cost an additional $458 billion according to the Congressional Budget Office. Of the billions spent for deployment of security systems and for military operations, only a small fraction of that amount goes for personnel with the expert analytical and investigative skills needed to formulate plans to neutralize terrorist operations before they are carried out.

How much does the United States spend overseas annually in nonmilitary areas to combat terrorism? The data are elusive, but for fiscal year 2004, the GAO put the figure at $11 billion. Clearly this is not where the nation's counterterrorism priorities currently lie. Should more, perhaps, be allocated to diplomacy?

The costs of terrorism to the world economy are even more staggering. In the aftermath of September 11, 2001, costs were estimated to be between $33 billion and $36 billion. Osama bin Laden has claimed the increased costs to the global economy as a result of perceived increases in risks after September 11, 2001, to be $1 trillion. A Congressional Research Service report by a colleague—Dick Nanto—confirms the estimate.[2]

We are engaged in an ongoing campaign, not a war in the traditional sense. Our government is heavily committed to this open-ended ongoing effort. Not to be thus engaged would be to neglect a core element of the social contract between government and the governed: the public's need for security. Key here is the ability to sustain a long-term campaign. This takes international cooperation. Levels of international cooperation are an important metric in measuring progress against terrorism. Past threats have often united the United States and its allies. Today the threat of terrorism often divides us.

---

[2]Nanto, D. K. 2004. 9/11 Terrorism: Global Economic Costs. Congressional Research Service report RS21937, October 5, 2004. Washington, D.C.: Congressional Research Service.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

INCIDENTS

In terms of measuring incidents, we in the United States tend to define success in ways that make us feel most comfortable: body counts and other numbers. We are a Western, science and technology-oriented society. If we quantify a problem, we can handle it and solve it. However, a common pitfall is overreliance on quantitative data at the expense of its qualitative significance. In *Patterns of Global Terrorism*, incidents are statistically counted equally without regard to their broader impact. To the degree that terrorist constituencies are not from Western cultures, their mindsets do not place a premium on quantification. For instance, honor or revenge may be more important than numbers.

We define success by the absence of attacks. When the shooting or bombing stops, we are successful. Yet terrorists sometimes define success in terms of our expending limited resources trying to defend an enormous number of potential targets. For them, the absence of violent conflict may simply mean that they are focusing attention on economic, political, or social spheres, or just that they are in a waiting period. We define success in terms of the amount of money we confiscate from them. They define success in terms of the amount of money they force us to squander to seize potentially insignificant amounts.

ATTITUDES

In terms of attitudes, terrorists see success as breaking our will and that of our allies. They want to win the conflict in the political arena on the streets of Washington, D.C.; London; Paris; Karachi; Moscow; and Madrid. They want our public to tire of the casualties caused by terror in places such as Baghdad, Chechnya, and wherever else terrorists can strike a blow. They want our public to push our governments to adopt policies of oppression, or alternatively, of appeasement. They may see U.S. public opinion concerning antiterrorism policies as our vulnerable point, counting on a protracted Vietnam-war-type reaction of protest.

Other criteria we might place in "attitudes" include the

- negative psychological or behavioral impact of terrorism on society
- loss of public confidence in governments or in their security measures
- degree to which terrorists can radicalize and polarize Islam against the West and vice versa
- level of anti-U.S. or anti-Western sentiments
- level of religious bigotry in countries that are breeding grounds for terrorists

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TRENDS

In terms of trends, the criteria might include

- the number of governments that do not embrace appeasement policies
- the number of defectors from the terrorist ranks
- the terrorist's level of Internet activity, including the number of Web sites and use
- the amount of media coverage they receive
- the number of supporters and recruits they gain

A related issue here is how our policies affect popular support and recruiting. For example, we entered Iraq, anti-U.S. sentiment skyrocketed; when we rescued tsunami victims, pro-U.S. sentiment jumped in Indonesia.

The issue of momentum is important as well. Is there a point at which an ideological movement loses momentum and falls apart? Is this the bottom line we aim for?

In conclusion, let us ask: Are we making progress? What is progress, and equally important, what is not progress? How do you suggest we define progress or the lack thereof? I look forward to your questions and comments.[3]

[3]Since the delivery of this presentation, the author has completed a more detailed study on this topic. See Combating Terrorism: The Challenge of Measuring Effectiveness. Congressional Research Service report RL33160, available on the U.S. Department of State Web site at http://fpc.state.gov/documents/organization/57513.pdf.

Copyright National Academy of Sciences. All rights reserved.

On Efforts to Counter International Terrorism in the Russian Federation and Possible Areas of U.S.-Russian Cooperation in this Area

Valentin A. Sobolev
National Security Council of the Russian Federation

Allow me first of all to express my thanks for the invitation to speak at such a representative meeting of scientists of the United States and the Russian Federation.

I feel it is important to note that we have all been brought here by a desire to sum up the results of our joint activities, plan new measures taking into account the real situation in the struggle against international terrorism, and expand our cooperation by improving its effectiveness. The atmosphere prevailing here is fully conducive to a confidential discussion and an informal yet businesslike and constructive exchange.

In analyzing trends in the evolution of terrorism, attention should be focused on the following basic parameters by which its danger to society has increased:

- Growth rates—More than 10,000 terrorist acts have been committed worldwide during the past three decades.
- Level of organization—During the past century, terrorism has developed from the level of lone terrorists and small terrorist groups to transnational terrorist associations like al Qaeda.
- Material-technical and financial support—Terrorists' resources have evolved from the dagger and the pistol to colossal explosions and the possible use of weapons of mass destruction; from modest financial resources to funds in the millions, obtained through the laundering of criminal proceeds and through sponsorship support from religious and nationalist organizations.
- National and transnational scales of terrorist activities—Terrorism is moving from crimes in a single location to the seizure of entire cities, countries, or regions.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- Degree of severity of consequences and number of human victims—The rates of increase in the numbers of casualties are averaging an order of magnitude higher than the rates for the number of terrorist acts.
- Nature and scope of goals—Terrorist acts range from the murder of individuals to the overthrow of legitimate governments, the destruction of states, and the practical elimination of entire peoples.
- Expansion of the social base for terrorism—Not only individual organizations and political, nationalist, and religious organizations but also entire populations who are often deluded and significant segments of populations are lining up under the banner of terrorism.

Terrorism in our times is also characterized by the presence of ready forces equipped at the highest technical level. Terrorists are attempting to use the latest scientific and technical achievements for their criminal purposes. There is no doubt that terrorism is today one of the primary threats to the security of the entire world community.

In recent history, Russia has been among the first to really feel this threat. Suffice it to recall that in 1995, at the G-8 meeting in Ottawa, the Russian delegation warned that the world community needed to pay attention to the increased level of activity on the part of international terrorism, particularly in the North Caucasus region. Unfortunately, however, our calls to join forces in the struggle against terrorism were not heard in time.

For us, Chechen terrorism continues to be one of the primary instruments of international terrorism operating in Russian territory and even represents a sort of testing ground for the use of cutting-edge technologies in terrorist acts.

One example is the terrible tragedy in the city of Beslan, North Ossetia, which I would classify as comparable in its scope, severity, and consequences with the events of September 11, 2001, in New York City. The actions of the terrorists were directed against children with the aim of destabilizing the situation in the North Caucasus region.

There is sufficient evidence that bandit groups operating in Chechnya and other Russian regions have ties to international terrorism. It is sufficient to recall that mercenaries from more than 50 states were found to be participants in the zone of the counterterrorist operations in Chechnya. Prominent roles were played by members of al Qaeda, including Abu al-Walid, Abu Kuteida, and Marwan Idr. According to our information, even today there are 150 to 200 foreign mercenaries in the bandit groups in the Chechen Republic.

Absolutely analogous to the training camps in Afghanistan and Pakistan, training bases for fighters, including individuals from many foreign countries, were operating in the Chechen Republic from 1994 through 1999. Meanwhile the spiritual leader of the Chechen bandits, Zelimkhan Yandarbiev, was a frequent guest of the Afghan Taliban leadership, receiving ideological and material support.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

The Khasavyurt peace accords of 1996, under which the Chechen leadership at that time committed to disarming the bandit groups and establishing order in its territory, were in fact used to prepare an armed expansion. The result was an act of open aggression by international terrorism against Russia. In August 1999, well-armed bands of mercenaries trained in the camps invaded the territory of the Republic of Dagestan. Their purpose was to detach a portion of Russian territory from the Black Sea to the Caspian Sea to create a World Arab Caliphate, an idea born in the depths of al Qaeda.

It must be recognized that in the three-and-one-half years since the terrorist attacks in New York City and Washington, D.C., the world community has done a great deal to establish effective partnership in countering international terrorism. An international antiterrorist coalition has been formed. The role of the United Nations and its Security Council has increased, and in our opinion these organizations can and must become the primary bodies uniting the efforts of all countries of the world in the fight against terrorism.

As for Russia, as President Vladimir Putin has declared, we consider the task of strengthening the antiterrorist coalition to be among the most important tasks it faces. Our position is well known: The time has come to reject double standards with regard to terror, regardless of the slogans behind which it might take cover. Those who killed the children in Beslan and seized the planes for the attacks on the United States are entities of the same breed. The provision of asylum to terrorists, their accomplices, and their sponsors in violation of agreements that have been made undermines the unity and mutual trust of participants in the antiterrorist front, serves as justification for the terrorists' actions, and in fact encourages them to commit the very same crimes in other countries. Attempts to use the struggle against terrorism for various types of geopolitical games are even more counterproductive and dangerous. Any concession to terrorists is a signal that they can achieve their goals and an incentive for them to commit new crimes.[1]

The inhumanity of the recent terrorist acts speaks of the need to ensure reliable guarantees that terrorists will not be able to gain access to weapons of mass destruction (WMD). Russia is prepared for the closest international partnership on this question. Our country is one of the initiators of UN Security Council Resolution 1540, a participant in the Proliferation Security Initiative, and a coauthor of the G-8 action plan on nonproliferation. In our view, strict and unwavering fulfillment by all countries of their obligations under the relevant

[1]For example, on March 11, 2004, approximately 200 people were killed in a series of bombings in Madrid. More than 1,800 people were injured to varying degrees, and as another result of the bombings, a new government also came to power two weeks later. The terrorists instantly connected these two events. Later, after a hostage was seized, Spain removed its military forces from Iraq. The terrorists again announced their achievement, and the number of seizures of hostages from other countries increased many times over.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

conventions banning these types of weapons must be a reliable barrier against the spread of chemical and biological weapons.

One of the myths widely discussed in the West with regard to Russia states that, first, nuclear weapons and their components are poorly protected in our country and that the Russian mafia has virtually free access to them. Second, conservatively inclined military officers, representatives of the special services, and the military industry are supposedly secretly supplying other countries with WMD components or technologies that are prohibited for export. Since the moment that the Russian Federation appeared as a state, no instance of the disappearance of even one gram of weapons-grade uranium or plutonium has been recorded. This mythology of Russia as a malevolent proliferator is not only supported in film thrillers and pseudoanalytical articles appearing in a number of Western media outlets but also is being used by speculators to turn a profit. For example, cases have been recorded in Afghanistan in which containers with technical markings in Russian and supposedly containing weapons-grade uranium have been offered on the black market.

The growing drug trade is closely linked with terrorism. The cancer of international terrorism is spreading relentlessly around the globe. In some places it is just beginning to find a base, while in others it has already managed to put down deep roots. This primarily pertains to the so-called instability belt, which extends from the Philippines and Indonesia through the Indian subcontinent, Central Asia, the Caucasus, and the Middle East to the Serbian territory of Kosovo.

If we look carefully at a geographic map, we may discover a surprising coincidence between this terrorism belt and the drug-trafficking route most convenient for the shipment of drugs into Europe: from the region of the Golden Crescent (Afghanistan, Pakistan) through Central Asia and the Transcaucasus and further along the so-called Balkan, or northern, route. The flow of drugs from Afghanistan has taken on a global character. We note with alarm that the efforts of the international community and the Afghan authorities to counter the production and contraband sale of drugs have not yet produced the necessary effect.[2] The problem is sufficiently acute, and much depends on its resolution, including the success of the struggle against terrorism; fulfillment of the program for disarmament, demobilization, and reintegration of the fighters involved in irregular formations; and ultimately the creation of a stable centralized government in Afghanistan. One would like to see the International Security Assistance Force play a more active role in the war against drug production and trafficking.

[2]According to estimates from the UN Office on Drugs and Crime, Afghanistan produced 87 percent of the world's opium supply in 2004 (in 2003, 76 percent). A total of 4,200 metric tons of opium was produced (in 2003, 3,600 metric tons). The area under poppy cultivation reached 131,000 hectares (in 2003, 80,000 hectares). Overall, the opium economy employs about 2.3 million people. The volume of income earned by producers and drug traffickers is estimated at 2.8 billion dollars.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Efforts to build cooperation among special services and law enforcement agencies require special attention, and we believe that this issue must be raised to a qualitatively new level of trust and coordination of actions. The December 2004 visit to Russia by U.S. Federal Bureau of Investigation (FBI) Director Robert Mueller is graphic evidence of this. Russian Federal Security Service Director Nikolai Patrushev and the FBI director signed a memorandum on cooperation between the special services of the two countries in the fight against international terrorism and the spread of weapons of mass destruction, along with a number of other agreements.

I would now like to say a few words about the state system for countering terrorism in Russia. The outlines for the formation of this system are set forth in the Constitution of the Russian Federation and by the federal laws On Security, On the Struggle Against Terrorism, On States of Emergency, On Countering the Legalization of Profits Obtained by Criminal Means and Used to Finance Terrorism (Money Laundering), and a number of others.

The president of the Russian Federation heads the state system for countering terrorism and determines the fundamental elements of state policy in this regard, either directly or through the Security Council of the Russian Federation. The government of the Russian Federation coordinates counterterrorism efforts undertaken by federal executive-branch agencies and organizes support for them with the necessary forces and resources. The Federal Antiterrorist Commission, which is chaired by the prime minister, handles overall coordination of the activities of federal executive-branch agencies in countering terrorism. Regional antiterrorist commissions also operate in the various entities that make up the Russian Federation. The lead agency, with functions including the detection, prevention, and suppression of terrorist activities, is the Federal Security Service of the Russian Federation. The list of agencies whose forces and resources are involved in antiterrorist activities also includes the Ministry of Internal Affairs, the Foreign Intelligence Service, the Ministry of Defense, and the Federal Financial Monitoring Service.

The situation in the North Caucasus has an objective impact on the need to improve the state system for countering terrorism. In late 1994 the country's leadership set itself to the task of eliminating the incipient conflict in Chechnya and reestablishing constitutional order in the republic. This was not achieved. Furthermore, active efforts were initiated to detach Chechnya from Russia. Unfortunately, political will was not displayed in that period and a realistic assessment was not made of the events that were occurring. The striving of the extremist leaders to label the conflict as international and to involve international forces in its elimination was not taken into account. From 1996 to 1999 these circumstances allowed the Ichkerian leaders to create large, illegal, armed terrorist formations in the republic and to begin an invasion of the territory of the neighboring Republic of Dagestan with the aim of taking it over. In response a counterterrorist operation in the North Caucasus was announced by a decree of the

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

president of the Russian Federation in accordance with existing legislation. The goal of the operation was to liquidate the illegal armed bandit formations, restore the legal rights and freedoms of the region's population, eliminate separatism, and prevent the spread of terrorism to other regions of Russia.

Three basic stages of the counterterrorist operation may be highlighted. The first stage was military (1999–2001), and began with the start of the terrorists' aggression against Chechnya's neighboring republic, Dagestan. The military stage was characterized by the actions of primarily the armed forces and the widespread use of arms to oppose large and well-organized armed bandit formations. Leadership of the military stage of counterterrorist operations was undertaken by the Ministry of Defense.

Subsequently, following the destruction of major armed bandit formations, the special operations stage began (2001–2003). It was conducted under the overall leadership of the Federal Security Service. The goals of this stage were as follows: destruction of the organizational structure of the terrorist bandit organizations, neutralization of the bandit formations and their leaders, and closure of their funding channels. At the same time, efforts began to lay the foundations for creating organs of legitimate government in Chechnya and reestablishing the constitutional order.

The positive results achieved in stabilizing the situation in Chechnya and disrupting the centralized command structure of the bandit formations made it possible to move in 2003 to the third stage, which involved counterterrorist operations. The focus of actions was shifted to the law enforcement sphere. Leadership of the operations was assigned to the Ministry of Internal Affairs. This stage is currently being implemented by federal and republic-level forces and involves support for public security and order in the republic. These actions are being carried out in parallel with political processes under way in the republic and with restoration of the ruined economy. Increased powers are being transferred to the republic authorities. Having embarked on the path of peaceful development for their republic as a part of Russia, the Chechens themselves have begun working more actively to bring order to their homeland.[3]

[3]A legitimate government has been created in Chechnya. A president of the republic has been elected; the republic government and local governments are functioning. A referendum has been held in which the residents of the republic decided that it would belong to Russia as a subject. A constitution has been adopted; preparations are under way for parliamentary elections. The social sphere and the economy are being restored.

In 2004, population growth in the republic was among the highest in the region (about 102 percent). Average wage increases totaled 152 percent (one of the highest in the region).

Pensions are being paid, along with subsidies for children and the unemployed and monetary compensation for lost housing and property. In 2004, 39,000 families received monetary compensation for destroyed housing and lost property in the amount of about 14 billion rubles (from the federal budget).

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

The current situation in Chechnya shows a strong tendency toward stabilization. However, international terrorism has not cooled. It is forced to constantly find new ways to manifest itself that are even more dangerous for people. As has already been noted, it is international, and it seeks and finds support in international organized crime. It strives to obtain WMD and their components. It is terrible and merciless. The experience of the struggle against terrorism in Russia shows that the system that opposes terrorism must be constantly improved. Otherwise, we are doomed to defeat.

It is for this reason that the president of Russia has issued orders to improve the system for countering terrorism. To these ends the Russian Security Council is revising a draft Concept (Strategy) for National Security. The regulatory and legal base is also being improved. Plans call for radically changing the procedures for cooperation among all agencies involved in the struggle against terrorism, expanding their powers, and instituting accountability for failure to take measures to prevent terrorist acts. Also planned are increased criminal penalties for aiding terrorists and financing their activities and heightened controls over the production, sale, and use of explosives and weapons. Measures are being improved to ensure that the population receives timely notification regarding threats of terrorist acts and on the elimination of their possible consequences.

A great deal of attention is being focused on international cooperation. A preliminary analysis is under way about the expediency of bringing the national laws of Russia and foreign countries on the struggle against terrorism into compliance with a unified standard and about the question of creating a single international database on terrorist, separatist, and extremist organizations and their leaders and members. In our work we are also taking into account the practical

---

A total of 71 medical care facilities are operating, including the republic hospital and eight clinics. There are 65 kindergartens, of which 46 are located in rural areas. Two more kindergartens are being prepared to open.

Three higher educational institutions (with more than 20,000 students) and seven specialized secondary institutions (more than 6,000 students) are operating, along with 456 schools (with more than 14,000 teachers and 200,000 pupils), four boarding schools, and 95 continuing education facilities.

Active efforts are under way to restore the agricultural sector. Increases have been achieved in the number of livestock (by 120–160 percent), poultry production (140 percent), milk output (more than 200 percent), and the amount of grain milled (150 percent). The production of bread and bakery goods has increased by 120 percent. Housing and construction industry facilities are under construction.

The petroleum sector is developing. More than 2 million metric tons of oil is extracted annually, and sales of petroleum products have increased.

Television and radio broadcasting reach the entire territory of the republic. The telephone system has been restored. Thirty newspapers and six magazines have been registered and are being published.

Railway links to Moscow have been reestablished.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

steps taken by the U.S. leadership following the terrorist acts of September 11, 2001, to address problems of improving the effectiveness of protection of the nation's territory against the terrorist threat and preparing for actions in emergency situations.

In our view the range of measures that has been developed to improve interactions among all state agencies by creating new structures responsible for the country's security and reorganizing existing ones merits particular attention. We see the systemic approach of the United States in such areas as

- obtaining warning information about the likely location, nature, and methodology of potential terrorist acts
- stepping up border protection and ensuring the security of the transportation system
- protecting the most important elements of the infrastructure (key facilities)
- preventing terrorist organizations from gaining access to technologies and materials necessary to create weapons of mass destruction and preparing to eliminate the consequences of terrorist acts that might entail mass casualties among the population
- creating a national emergency response system

Regarding bilateral cooperation between our countries, I would highlight the following areas in which we should join forces first:

- timely detection and prevention of terrorist acts
- efforts to counter and operationally respond to emergency situations caused by the possible use of nuclear, biological, and chemical materials (this could also include wide-scale attacks in the information and communications sphere)
- the struggle against financing and other assistance for carrying out terrorist acts
- exchange of information, experience, and technologies and unification of standards in all spheres—legal, scientific, technological, and others
- study of the roots of terrorism's origins and of the organization of terrorists' motivational and ideological work on citizens and efforts to counter such phenomena

I would like to note that international terrorists have neither nationality nor religion. On the contrary, it is religion and national culture that now as never before require protection against the destructive impact of all sorts of extremism. A respectful dialogue is needed among various faiths and civilizations. With its ties to both the West and the East, Russia is prepared to play a role in this process, which is called upon to prevent the schism of civilization.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Of course, the aspects of antiterrorist activities that I have presented do not fully cover the entire range of problems associated with the study of terrorism, a range that will likely be augmented significantly from discussions at this workshop.

In conclusion, I would like to express my confidence that the joining of efforts by scientists from the national academies of the United States and Russia to address these problems will be fruitful and to wish you success in this difficult but extremely important and responsible endeavor.

Copyright National Academy of Sciences. All rights reserved.

Cybercrime and the Training of Specialists to Combat It in Russia

Nikolay V. Medvedev
Department of Information Security,
Bauman Moscow State Technical University

THE INTERNET AND CYBERCRIME IN RUSSIA

The present stage of human development is characterized by the explosive growth of information technologies, a historically unparalleled situation that is irreversibly changing people's way of life. All previous key inventions such as the telegraph, telephone, radio, television, and computer only paved the way for the unprecedented integration that is under way. In our times, global cyberspace—the worldwide Internet—simultaneously represents a repository for a colossal amount of information, a means of global broadcasting, and a medium for cooperation and human communication encompassing the entire world. The Internet is not controlled by any state structures. According to the predictions of the public organization the Internet Society, in 2005 the number of Internet users in the world will exceed one billion, of whom about seven million will be from Russia.

Besides the multitude of positive aspects of this sort of global linkage and communication among individuals and peoples, information technologies significantly expand the arsenal of means and capabilities of criminals. Any country with computers and Internet access could, intentionally or not, become a base for users with evil intentions, any one of whom could have the goal and motivation to inflict criminal harm on other people and organizations. These people have global cyberspace at their disposal to use for criminal purposes. Crimes of such a nature are called cybercrimes (in Russian legislation, crimes in the sphere of computer information), and the people who commit them are generally called cybercriminals. Although the term cybercrime is not legally formulated in Russian legislation, this concept has taken firm root in practice.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Cybercrime may include the following:

- unauthorized access to information
- creation, use, and dissemination of harmful computer programs, including over the Internet
- intentional disruption of the normal operation of computers and networks
- illegal trade in equipment for capturing computerized information
- falsification of documents with the use of computer technologies
- distribution of counterfeit software
- conduct of financial swindles
- publication of calls for violence and terror
- publication of Nazi and fascist propaganda

The main characteristic of these crimes is that, as a rule, they have no physical signs.

Cybercriminals currently use various types of network attacks. Some use computer viruses, including network worms, which modify and destroy information or block the operation of computer systems; logic bombs, which are triggered under certain conditions; or Trojan horses, which send various types of information from infected computers back to their masters over the Internet.

The weapons of cybercriminals are being constantly honed, and their means of conducting information attacks are becoming increasingly refined. In the long term, we can expect to see the appearance of new nontraditional types of network attacks and computer crimes.

On the whole, we can state with confidence that the material damage from crimes in the information technology sphere is measured in the billions of U.S. dollars and is increasing with each passing year. Furthermore, the expected growth in financial losses from criminal infringements is based not only and not so much on the increased number of computer attacks as on the growing scale of the use of network information technologies in business. In the face of harsh competition, companies are forced to shift a large portion of their business communications onto the Internet, which makes them vulnerable to criminals unless matters of information protection are handled appropriately.

The world community has fully realized the potential consequences of the threat of cybercrime, and in this regard representatives of the European Union member states, the United States, Canada, and Japan signed the International Convention on Cybercrime in November 2001. In the convention, crimes committed in the information environment or against or with the aid of information resources are in fact defined as cybercrimes.

With the far lower level of development of computer networks in Russia, the situation in the Russian Federation is obviously not yet as serious as in the United States, but its intensity is increasing from year to year. We are increasingly sensing how the modern information criminal is becoming a reality.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

The Criminal Code of the Russian Federation includes articles establishing penalties for computer crimes and a chapter defining crimes in the computer information sphere. This chapter includes three articles setting forth penalties for illegitimate access to computer information (Article 272); the creation, use, and dissemination of harmful programs via computer (Article 273); and violation of the rules of operation of computers, computer systems, and networks (Article 274). The number of crimes committed under these articles is increasing each year. Meanwhile, the number of crimes discovered is also on the rise. Let us look at the facts.

In 2004, 4,523 computer information crimes were discovered in the Russian Federation. Of these, 3,944 fell under Article 272 of the Criminal Code and 577 under Article 273. During this past year, the Russian Federation significantly stepped up its efforts to stop the distribution of unlicensed software, thus making a worthy contribution to the world trend toward combating computer piracy. For example, 1,483 administrative violations were uncovered in the copyright area, and 216,635 compact discs with unlicensed software with a total value of more than 9 million rubles were confiscated by court order.

Like the rest of the world, the Russian Federation is currently facing the pressing problem of so-called spam, the mass distribution of electronic messages, largely advertising, that were not requested by their recipients. Receiving spam is like an invisible tax on all users of the Russian segment of the Internet. By various estimates, financial losses from spam vary from 120 to 200 million U.S. dollars per year. In 2004 a precedent for combating this type of crime was created for the first time in the Russian Federation, with the first conviction of a spammer under the law. This person had created a computer program, sendsms.pl, and sent 15,000 mobile phone subscribers text messages with uncensored content smearing the business reputation of a cellular communications company.

Also arising last year was a trend for the use of the Internet as an auditorium to shape public opinion and exert pressure on private individuals and officials by spreading information damaging honor and impugning dignity or by disseminating citizens' personal or family secrets. In one example the authorities halted the activities of a perpetrator who had posted an Internet site with intentionally libelous materials regarding the president of the Russian Federation and statements insulting his honor and dignity. Obviously, negative press technologies adopted from the media have begun to be used on the Internet. Furthermore, in trying to evade responsibility, the ill-intentioned are claiming that laws regulating media activities do not apply to the Internet, even though its audience is often greater than that of many print publications. The Russian Federation is working actively to standardize the legislative and regulatory base for these violations, while maintaining a lack of government censorship.

An analysis of personal information about criminals arrested in the Russian Federation in 2004 shows that computer crime is mostly perpetrated by adults.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Adolescents under age 20 comprise only 17 percent of the total number of criminals, the bulk of whom—70 percent—are persons between the ages of 20 and 35. It should also be noted that 63 percent of these persons attended or graduated from university, which reflects the high intellectual level of this criminal activity.

No crime, including cybercrime, can occur on its own. Crimes are committed by criminals, and in this case, by cybercriminals. People can have different motives for committing crimes. Determining the boundary between crime and terrorism in cyberspace is possible simply by determining the goals of cyberterrorism. In practice, these goals coincide with the goals inherent in terrorism in general and political terrorism in particular. One may state that every terrorist is a criminal, but not every criminal is a terrorist.

According to the common definition of terrorism, it is a conscious and directed use of violence or the threat of violence to force society, the state, or the government to comply with the political, ideological, religious, or economic goals of the terrorist organization. A terrorist act is a crime aimed at having an emotional impact on public opinion, engendering fear and panic in society, evoking distrust of power structures, and ultimately destabilizing the political-economic situation in the country. This is a crime aimed against the security of society, the state, and each individual citizen. The cyberterrorist substantially differs from the hacker, computer hooligan, thief, or swindler. The main element of the cyberterrorist's tactics is to ensure that the crime has maximally dangerous consequences and broad public resonance and creates an atmosphere that threatens repetition of the terrorist act without specifying a specific target of attack.

The experience of the Russian Federation shows that the motives of cybercrimes are changing. Whereas computer crimes in the past were committed mainly by adolescents motivated by hooliganistic or experimental considerations, motives of greed now predominate. Intentionally false reports of terrorist attacks represent an exception. In particular, specialists have established that this was the motive of the Russian student who disseminated information about a planned New York subway bombing, accompanying his message with the words "Allahu akbar."

TERMINOLOGY USED IN THE RUSSIAN FEDERATION FOR CLASSIFYING THREATS AND MEANS OF COUNTERING CYBERATTACKS

There is no commonly accepted terminology in the sphere of information security for computer systems and networks, which makes it necessary to define certain fundamental concepts (as they are used in the Russian Federation).

Threat—A potential event, action, or process that by its effects on network components could lead to the infliction of material, moral, or other damage on network resources.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Vulnerability—Any characteristic or property of an information system that if used by an intruder could lead to realization of a threat—in other words, weak points in systems.

Attack (intrusion)—An event in which a perpetrator or intruder attempts to access a system or commits any sorts of abuses with it, or any action by an intruder leading to realization of a threat by means of attacking vulnerabilities. An intruder carries out an attack in three stages: (1) collection of information about the network to be attacked, (2) implementation of attack, and (3) completion of attack. Traditional means of countering intrusions come into play only in the second phase of attack implementation. Such a situation helps to increase the damage from the attack. It would be more logical to begin active response efforts at the first stage of the attack. The most obvious example would be an attack aimed at implementing a threat to deny services or to deny access to information (a denial-of-service attack). This sort of attack is extremely difficult to thwart at the implementation stage, so it would be reasonable to suppress it at the first step in its development.

Intrusion detection—A range of methods intended to detect an intrusion (attack) on a network by means of observing various parameters, events, and subsystems for registration and network monitoring.

Intrusion detection system—A range of software and hardware network resources intended to detect intrusions (attacks).

In addition to the denial-of-service attack, which stalls a server by placing an increased load on its central processor, there are many harmful programs called viruses, which affect individual computers, computer systems, networks, and, recently, mobile communications resources, using a developed operating environment and elemental base. The number of viruses is constantly increasing, reaching 25,000 according to estimates in late 2004. Table 1 presents a brief classification of current viruses as categorized in the Russian Federation.

With corporate and local networks and individual users accessing the Internet, one of the most complex problems is that of ensuring the security of information resources. A number of technologies are employed to address this problem, each of which is designed to protect against a particular class of potential security threats. These include intrusion detection systems, public key infrastructure, virtual private networks, antivirus software, cryptographic systems, identification and authentication systems, security scanners, and so forth. Firewalls hold an important place among these technologies, and their adequate application can substantially reduce risks associated with unauthorized access to data. However, comprehensively deterring cyberthreats is possible by developing optimal information security policy consisting of a combination of passive and active methods of applying protection technologies.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 1 Classification of Current Viruses

Group	Type	Characteristics
Environment	Network viruses	Spread through various networks, that is, during transmission of data between computers connected by a network.
	File viruses	Infect executable files and are loaded after start-up of the program in which they are located. File viruses can also be embedded in other types of files, but if they are placed in nonexecutable files, they do not obtain control and lose the capacity to spread.
	Boot viruses	Install themselves into the boot sector of physical or logical discs containing boot programs.
	Mobile communication system viruses	The newest type of virus. They infect the operating environment of the latest generation of mobile telephones, which have broad intellectual capabilities.
Means of infection	Resident viruses	Leave a resident code in operating memory that intercepts communications between the operating system and infection targets (files, boot sectors of discs, and so forth) and installs itself in them. Resident viruses live in memory and remain active until the computer is turned off or rebooted.
	Nonresident viruses	Do not infect computer memory and are active for a limited time. They are activated at certain times, for example, when documents are processed with a text processor.
Destructive potential	Not dangerous	Reduce memory volume; do not disrupt the computer operations; produce graphic, audio, or other effects.
	Dangerous	Can cause various disruptions in computer operations, for example, locking up or incorrect printing of documents.
	Very dangerous	Can cause losses of programs and data and deletion of information in system memory sectors and can even cause a breakdown of moving parts of the hard disc.

THE TRAINING OF HIGHLY QUALIFIED INFORMATION SECURITY SPECIALISTS IN THE RUSSIAN FEDERATION

Only a major leading university with the appropriate educational, methodological, and technical base is capable of training highly qualified specialists able to accomplish the task of ensuring comprehensive information security. The educational objectives for specialists of this type at Bauman Moscow State Technical University are as follows:

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- theoretical foundations for the engineering-technical protection of information
- methodological support for the engineering-technical protection of information
- creation and operating principles of information systems and networks (ISN)
- methodologies for designing, building, and operating secure ISNs
- criteria and methods for evaluating the security of ISNs
- means and methods of unauthorized access to ISN information
- architecture of protected computer networks
- software, hardware, and technical means of creating protected networks
- principles of building and managing protected networks
- rules for the organizational, technical, and legal protection of information
- use of software and hardware technologies for protecting information
- construction and operation of protected databases
- systematic approach to the problem of protecting information in database management systems
- mechanisms for protecting information in databases and database management systems and opportunities for overcoming them
- conceptions of the engineering-technical protection of information
- physical foundations for the engineering-technical protection of information
- organizational foundations for the engineering-technical protection of information

As a result of their training in this discipline, specialists must understand the following:

- promising areas for the development of computer security theory
- methods for analyzing information security threats
- architecture of secure ISNs
- principles for constructing secure systems
- typical attacks on secure ISNs
- promising areas for the development of network security technologies
- current problems in information security science and the role and place of information protection in networks when addressing comprehensive information security problems

They must know the following:

- methodological and technological foundations of comprehensive security for ISNs
- threats and methods of violating ISN security

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- formal models lying at the foundation of ISN protection systems
- standards for evaluating ISN security and their theoretical foundations
- methods and means of building and operating secure ISNs
- methods and means of verifying and analyzing the reliability of secure ISNs
- methodological and technological foundations for ensuring the information security of network-automated systems
- threats and methods of violating the information security of network-automated systems
- physical processes in technical means and systems that lead to leakage of secure information
- typical models of attacks aimed at overcoming the protection of network-automated systems, conditions under which they might be carried out, possible consequences, and means of prevention
- role of the human factor in ensuring network security
- possibilities, means, and rules for applying basic software and hardware means of protecting information in networks
- principles for the operation of basic secure network protocols
- foundations for the application of firewalls for network protection
- rules for setting network security policy
- standards for evaluating secure network systems and their theoretical foundations
- methods and means of designing, constructing, and evaluating secure network systems
- conception of the engineering-technical protection of information
- basic principles and methods of information protection
- basic guiding and regulatory documents on the engineering-technical protection of information
- procedures for organizing the engineering-technical protection of information

They must know how to

- analyze ISNs from the standpoint of ensuring computer security
- develop security models and policies using well-known approaches, methods, means, and theoretical foundations
- apply standards for evaluating the security of ISNs in analyzing and designing information security systems for them
- implement information protection systems in ISNs in accordance with standards for evaluating ISN security
- analyze network automated systems from the standpoint of ensuring information security

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- develop network security models and policies using well-known approaches, methods, means, and theoretical foundations
- apply standards for evaluating secure network systems in analyzing and designing systems to protect information in automated systems
- apply secure protocols and firewalls necessary for implementing information security systems in networks
- take measures to counter network security threats using various software and hardware means of security in accordance with rules for their application
- create information security systems in automated systems in accordance with standards for assessing system security
- identify threats and technical channels for information leakage
- describe (model) security targets and information security threats
- apply the most effective methods and means of engineering-technical protection for information
- monitor the effectiveness of security measures

They must have the following skills:

- work with ISNs for distributed computing and information processing
- work with ISN documentation
- use of criteria for evaluating ISN security
- construction of formal models of ISN information security systems
- construction and operation of computer networks
- design of secure networks
- comprehensive analysis and evaluation of network security
- work with means of interface support with various categories of database management system users
- work with database management systems on various platforms
- develop and manage databases
- work with means of ensuring database management system integrity
- work with means of ensuring database confidentiality
- work as database security administrator
- device-based evaluation of the energy parameters of side radiation from technical means and systems
- engineering calculation of the parameters of the controlled zone

By completing their studies at the university, the specialists acquire theoretical information and practical skills in combating computer terrorism and can independently develop enterprise information security policies based on comprehensive integrated solutions, conduct scientific research, and develop new methods for countering cybercrime.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

CONCLUSIONS AND RECOMMENDATIONS

Cybercrime is not restricted to crimes committed on the Internet. It extends to all forms of crimes committed in the sphere where information, information resources, and information technology are the targets, means, or tools of crime. With the current growth of cybercrime, which presents a danger to people's lives and welfare, threatens the security of all states, and undermines trust in government institutions, it is vitally important to ensure protection against this type of criminal activity. Therefore, we currently need to enhance the level of international coordination of scientific research on preventing and countering acts of cybercrime.

First, we need to conduct scientific research on developing a single conceptual framework. We must develop and amend legislative, regulatory, and legal documents for this type of crime, including those governing international activities. Studies on creating modern technologies for detecting and deterring network attacks and neutralizing criminal impacts on information resources are of the highest significance. In order to accomplish this, we need to develop plans for joint research on countering cybercrime. Themes for such plans could include the following:

- organizing exchange programs for undergraduate and graduate students, instructors, and researchers in the leading higher educational institutions of the Russian Federation and the United States
- creating a single conceptual framework, terms, and definitions regarding the development of means and systems for countering cybercrime and cyberterrorism
- creating a set of recommendations for government legislative organs on studying and amending regulations and laws regarding this type of crime, including those governing international law enforcement activities
- creating modern theoretical methods and applied technologies for detecting and deterring network attacks and neutralizing criminal impacts on information resources

Copyright National Academy of Sciences. All rights reserved.

Methodology for Assessing the Risks of Terrorism

Nikolay A. Makhutov
Institute of Mechanical Engineering of the Russian Academy of Sciences

INTRODUCTION

Through the efforts of specialists from many countries, a broad scientific base has now been created for analyzing and classifying the risks of extreme situations of a natural and *technogenic* nature, studying scenarios by which they might begin and develop, and reducing the vulnerability of high-risk sites with regard to natural and technogenic disasters.[1] This scientific base must be used as widely as possible in efforts to ensure security against the impacts of terrorism.

This approach to analyzing terrorism-related risks presupposes that emergency situations initiated by terrorist acts develop according to laws analogous to the development of ordinary emergency situations caused by natural or industrial disasters. Therefore, they may be analyzed using methods and models used in addressing classical problems in risk and safety theory.

The threat of terrorist acts must be included in the system of studies of possible scenarios of how emergency situations might develop. In particular, event trees used in risk analysis at critically important infrastructure sites must be augmented with scenarios taking into account possibilities of terrorist attacks, which substantially change the scenarios themselves as the structure of primary initiating factors in emergency situations. They also lead to the creation of cascading processes in the development of accidents and catastrophes with the most serious losses to the population, economic objects, and other vital resources.

[1]Knowledge International Humanitarian Fund. 1998-2003. Russia's Safety: Legal, Socioeconomic, and Scientific-Technical Aspects 1-24. Moscow: Znanie Publishers. See also: Problems of Safety and Emergency Situations: Scientific-Technical Journal. 1998–2004.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

We need to include the analysis of terrorism risks and terrorist mechanisms for initiating extreme situations in the range of problems being considered. This requires developing and adapting existing models and methods for studying catastrophes so that they account for the special characteristics of their initiation by unauthorized and terrorist actions that could be taken to strike at the most vulnerable and significant targets critically important for the national security infrastructure.

In order to analyze risk and security with the possibility of terrorist actions, it is first necessary to compare the initiation stage of the extreme situation through terrorist actions and the changes and structure of impact factors of the terrorist act with those in a traditional emergency caused by a natural or industrial disaster.

It should also be noted that the modern strategy for ensuring natural and industrial safety, which calls for focusing efforts not on eliminating the consequences of extreme situations but on predicting and preventing them, must also be extended to cover situations in which emergencies are triggered through terrorist actions. In this case, scientific developments regarding methods for managing the risks of terrorism must be accorded great significance in integrated risk management mechanisms.

CLASSIFICATION OF ACCIDENTS AND CATASTROPHIC SITUATIONS

The failure to provide for basic characteristics of reliability, resources, and safety regarding a range of criteria and reserve capacities leads to the possibility of accidents and catastrophic situations arising and developing at all stages of the creation and exploitation of complex technical systems. Over the past decade, institutes of the Russian Academy of Sciences and the Russian Ministry of Emergency Situations, Ministry of Industry and Science, State Mining and Industrial Inspectorate,[2] Atomic Energy Inspectorate, and Ministry of Education have synthesized a substantial volume of fundamental information on accidents and catastrophes of an industrial, natural/industrial, and natural character as part of the State Scientific-Technical Program for Safety for the Population and Economic Objects Considering the Risk of Natural and Industrial Disasters (SSTP Safety). In carrying out this program, participants analyzed and generalized information on the basic characteristics, conditions, and scenarios for the outbreak of accidents and catastrophes in the natural and industrial spheres engendered by complex dangerous phenomena and processes in various regions of the world. Potentially dangerous facilities and natural processes might create catastrophes in the

[2]Translator's Note: On March 9, 2004, Gosgortekhnadzor was transformed into the Federal Technological Inspection Service. On May 20, 2004, the latter was transformed into the Federal Ecological, Technological, and Atomic Inspection Service.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

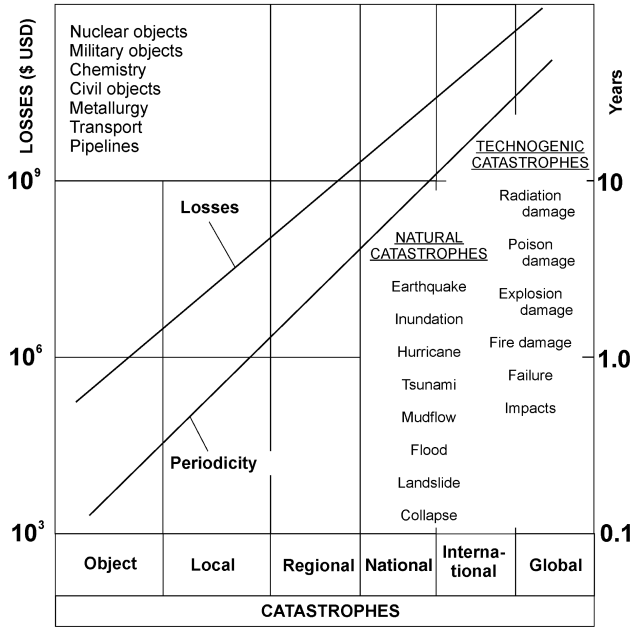


FIGURE 1 Losses and periodicity of natural and technogenic catastrophes.

following classes: planetary, global, national, regional, local, facility-level, and localized (Figure 1). The potential damages and periodicity of occurrence were evaluated depending on the class of accidents and catastrophes (beginning with global and ending with localized).

Official documents in the Russian Federation use six classes of catastrophes: transborder (equivalent to global), federal (equivalent to national), regional, local, facility-level, and localized.

Based on the results of this summary analysis, a classification of catastrophes was constructed, taking into account the damages U and the periodicity ΔT of their occurrence (see Table 1). Here the magnitude U for each catastrophe decreases from 1×10^{10} to 5×10^3 dollars, while the periodicity of their occurrence declines from 5×10^2 to 8×10^{-2} years. Thus the variation in damages (dollars per catastrophe) for various types of disasters could reach seven orders of magnitude, while that of the probability of occurrence $P = 1/\Delta T$ (1/year) could reach three orders of magnitude.

The concept of risk is the key one in resolving problems related to ensuring security. This paper includes a number of simplified equations that are used for assessing risks and risk factors. These include a basic equation for risk assess-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 1 Characteristics of Risks of Accidents and Catastrophes

No.	Class of accidents and catastrophes	P (1/year)	U (dollars)	R (dollars/year)
1	Localized	5.0×10^{0}	5.0×10^{3}	2.5×10^{4}
2	Facility level	1.2×10^{0}	4.0×10^{5}	4.8×10^{5}
3	Local	5.0×10^{-1}	7.0×10^{6}	3.5×10^{6}
4	Regional	1.6×10^{-1}	1.0×10^{8}	1.6×10^{7}
5	National	1.2×10^{-1}	1.5×10^{9}	1.8×10^{8}
6	Global	8.0×10^{-2}	1.0×10^{10}	8.0×10^{8}

ment (Formula 1), equations for assessing risk components (Formulas 7–13), and an equation for assessing risk management (Formula 14).

Risk is defined by means of the functional F_R of the probability that a catastrophe (natural or technogenic) will occur and the magnitude of the damage:

$$R = F_R\{P,U\} = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} P_i \cdot U_i = \int U(P) \cdot PdP = \int P(U) \cdot UdU \quad \text{(Formula 1)}$$

where R represents the risk associated with a natural or technogenic catastrophe; P, its likelihood; and U, its consequences (Formula 1).

The risks vary within the bounds of four orders of magnitude. For Russia the probability of the occurrence of national and regional natural-technogenic extreme situations differ by 1.4 times and are approximately an order of magnitude lower than the risk for local situations; the likelihood of local and facility-level accidents differs by 5 times.

The results of the studies that have been conducted have been reflected in the fundamental multivolume series *Russia's Safety*[3] and in issues of the journal *Problems of Safety and Emergency Situations*.[4]

The assessment of the probability P, damages U, and risks R of accidents and catastrophic situations involves a group of risk identification methods, including various methods for analyzing statistical information on natural and technogenic catastrophes of a particular type in the region being studied, as well as methods for analyzing the reliability of equipment and technological processes and the effectiveness of management and control. Methods for calculating the magnitude of damage substantially differ for various technical facilities and natural systems. Therefore, specialists in Russia and other countries are currently

[3]Knowledge International Humanitarian Fund. 1998–2003. Russia's Safety: Legal, Socioeconomic, and Scientific-Technical Aspects 1-24. Moscow: Znanie Publishers.

[4]Problems of Safety and Emergency Situations: Scientific-Technical Journal. 1998–2004.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

developing a group of special methods aimed at analyzing natural-technogenic processes capable of leading to accidents and catastrophic situations.

In assessing risk R in natural-technogenic-social systems, great importance lies in integrated (complex) risks, including the risks R_i from diverse factors operating on various temporal and spatial scales.

Integrated risks are determined by the specific nature of the interactions of the natural, technogenic, and social spheres. Terrorism could substantially change both the magnitudes of the risks R_i and R themselves and the nature of this interaction.

TYPES OF TERRORISM AND IMPACTING FACTORS

Modern terrorism may be divided into three types: traditional, technological, and intellectual (see Figure 2).

Traditional terrorism has been and remains aimed at the physical elimination (murder, abduction) of representatives of state and social structures and of average citizens to achieve certain social, economic, and political goals. In this case the actions of terrorists are directed against individuals and are carried out by organizing bombings, arsons, poisonings, kidnappings, and so forth. Here the

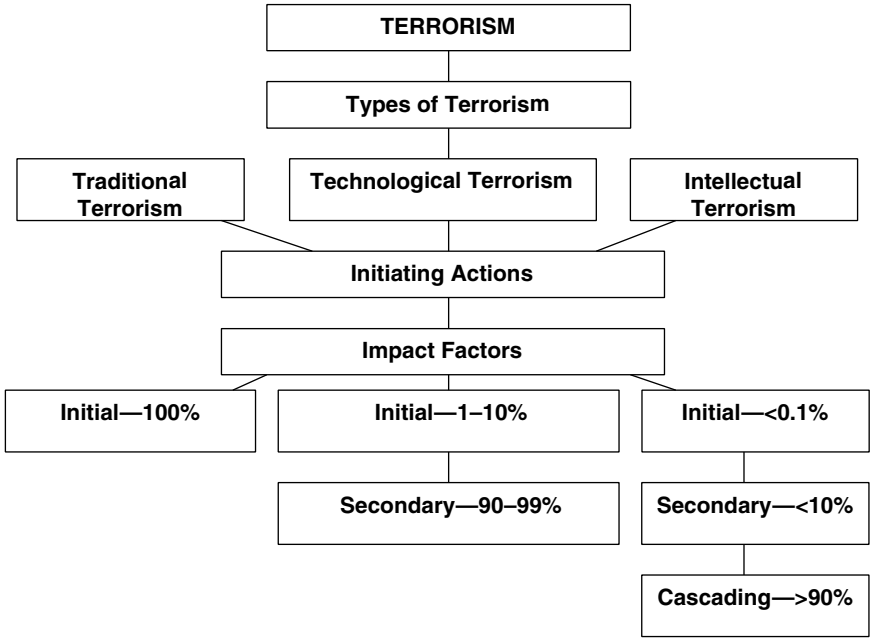


FIGURE 2 Types of terrorism and impact factors.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

fundamental damages are inflicted at the stage of the initial impacts of the terrorist acts.

Technological terrorism is represented by actions aimed against infrastructure targets critical to national security or committed using especially dangerous technologies, devices, and materials. With technological terrorism, the initial impact factors of the terrorist acts create technogenic accidents and catastrophes with a significantly greater (tens and hundreds of times) level of secondary impact factors that affect the targets attacked, their personnel, the population, and the environment. That is, in contrast to traditional terrorism, with technological terrorism the initial damages represent only an insignificant portion of the total damage compared with the secondary impact factors.

Intellectual terrorism is a type of terrorism in which the initial impact factors might be specially inserted in regulatory or technical documents and design engineering elements in the creation of new facilities in the technosphere or the operation of existing ones. These factors are capable of creating secondary impacts and damages leading to a cascade of tertiary impact factors.

The appearance and development of primary, secondary, and cascading impact factors of terrorism are subject to practically the same natural processes that shape traditional accidents and catastrophes at technosphere facilities that create extreme situations of a technogenic nature. This circumstance makes it possible to apply the scientific base developed for ensuring natural-technogenic security to addressing issues related to reducing the risks of terrorist impacts and countering terrorist threats.

In this regard the development of methods for analyzing the risks of terrorism and of means and systems for protecting against terrorist threats comes down to two basic problems:

1. reducing the risks R by preventing initiating dangers, threats, and challenges
2. reducing the risks R that extreme situations of a technogenic nature may develop if initiating factors do occur by redistributing a number of impact factors

FUNDAMENTALS OF DETERMINING THE RISKS OF TERRORISM

The theory of the security of complex social-natural-technogenic systems accords a substantial place to methods and means of analyzing crisis phenomena and processes, accidents, and catastrophes (their classification, potential dangers, and criteria base); basic scientific disciplines for describing scenarios regarding the occurrence and development of crises, accidents, and catastrophic situations; and comprehensive consideration of the interactions of the elements of the human/critically-important-object/environment system.

Comprehensive security determines the degree to which people, objects, and

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

the environment are protected against threats from various sources—from people themselves, from created and functioning complex technical systems, and from important natural impacts—in the occurrence and development of accidents and catastrophic situations.

Assessment of the potential danger of human actions by staff, unauthorized outsiders, and terrorists; high-risk facilities; and natural processes, taking into account various types of accident scenarios, must be carried out using the following three characteristic parameters: (1) accumulated energy reserves, (2) reserves of potentially dangerous substances (those presenting radiation, chemical, and biological hazards), and (3) information volumes and flows.

An important area of research in both overall catastrophe theory and terrorism risk assessment is the study of areas of dangerous and safe conditions, processes of damage accumulation, reactions of structural elements to external and internal effects, and development of maximal condition theory and especially of the process of postcritical behavior of system elements that leads to various consequences.

Taking into account a generalization of the basic factors involved in the occurrence of accidents and catastrophes, we may take the following as determinant:

- uncontrolled release of energy E (thermal, mechanical, blast wave, electromagnetic)
- uncontrolled release of the above-listed dangerous substances W
- uncontrolled dissemination or disruption of information flows I (management, informational, warning)

Given what has been outlined above, it is possible to construct areas of dangerous and safe conditions for various natural-technogenic-social systems (Figure 3) in which a situation could move into the danger zone in accordance with the laws governing random and determinate processes $v(t)$. The risks R_E, R_W, and R_I may be determined as follows in Formula 2 for each of the groups of catastrophe impact factors (E, W, I) based on Formula 1:

$$R = F_R\{R_E, R_W, R_I\} = F_R\{(P_E, U_E), (P_W, U_W), (P_I, U_I)\} \qquad \text{(Formula 2)}$$

The fundamental special feature of terrorism risks according to Figure 3 is that a common random process $v(t)$ is replaced on the radius-vector $r(t)$ by the nonrandom, directed selection of the direction $r(t)$ and time t_{TR} of the manifestation of the most dangerous damage factor characteristic of the given critical infrastructure site or natural process. In this case the catastrophe initiated by a terrorist act is realized on a substantially shorter time interval t_{TR} not linked with the time t_o needed to achieve a dangerous condition according to existing design norms and operating rules for the potentially dangerous facility. The time trajec-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

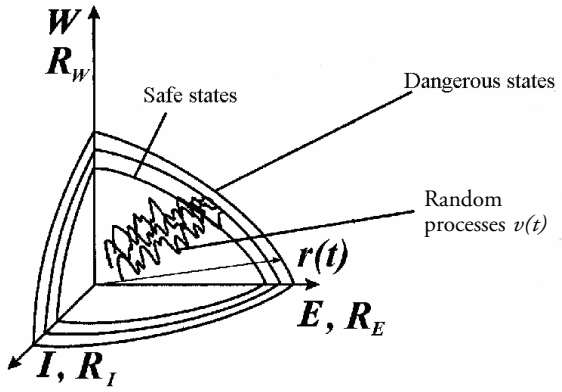


FIGURE 3 Areas of dangerous and safe states.

tory of the random process for regular functioning $v(t)$ becomes substantially longer than the time vector $r(t)$. Thus in analyzing the risks of terrorism, the determining correlations may be written as follows in Formula 3:

$$R_{TR} \geq R, \quad r(t) \ll v(t), \; t_{TR} < t_0 \qquad \text{(Formula 3)}$$

Four risk groups may be included in the overall risk structure R: systemic R_s, integrated R_i, differentiated (complex) R_d, and object (elemental) R_e. Here the risks in the previous group are elements of the following (Formula 4).

$$R_s = \sum R_i, \quad R_i = \sum R_d, \quad R_d = \sum R_e \qquad \text{(Formula 4)}$$

The risks of terrorism R_{TR} are components in all four risk groups. Each risk group can have its own corresponding level of management of the elements of national security: federal (R_s), regional (R_i), industrywide (R_d), and facility-level (R_e). Regarding critical infrastructure sites, the occurrence of accidents and catastrophes is associated with the realization of risks R_e; this subsequently has an impact on the entire further sequence of risks ($R_e \rightarrow R_d \rightarrow R_i \rightarrow R_s$).

Formula 1 may be used to monitor and forecast each of the types of risk listed.

If one analyzes the systemic risks of natural and technogenic catastrophes (or risks of extreme situations of a natural and technogenic character), then taking these into account in determining the probability of systemic threats using the functional $F_{PS,}$ we may write Formula 5 as follows:

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

$$P_S = F_{PS}\{P_N, P_T, P_O\} \quad \text{(Formula 5)}$$

where P_N is the probability of occurrence of an unfavorable event occasioned by the human factor, P_T is the probability occasioned by the status of objects in the technosphere, and P_o is the probability occasioned by environmental effects.

The form of the function in Formula 5 also remains the same for the probabilities of the realization of systemic P_s, integrated P_i, differentiated P_d, and facility-level P_e risks.

The significance here is that the role of the human factor in the assessment of P_s given changes in P_N is determined not only by the operators P_{NO} and personnel P_{NP} (as usually happens for P_d) but also by the individuals P_{ND} who are making decisions at all levels involved in state management of national and international security. The probabilities P_N, P_{NO}, P_{NP}, and P_{ND} comprise an interconnected complex that is also characteristic in the analysis of risks without considering terrorism.

$$P_N = F_P\{(P_{NO}, P_{NP}, P_{ND})\} \quad \text{(Formula 6)}$$

The probability of terrorism P_{NTR} as one manifestation of the human factor is a function independently included in P_N and is also connected with the actions of the operators, personnel, and managers.

$$P_N = F_P\{(P_{NTR}), (P_{NO}, P_{NP}, P_{ND})\} \quad \text{(Formula 7)}$$

The probabilities P_T are substantially dependent on the level of protection of the given critical infrastructure site from accidents and catastrophes. This protection is determined by the degree of degradation of the facility at a given stage of operation ($t < t_o$) with the level of diagnostic inspection and monitoring. Such a situation highlights the direct interrelation of the parameters P_T and P_N. Analogous to Formula 7, with acts of technological terrorism we may write the following:

$$P_T = F_P\{(P_{TTR}), (P_N)\} \quad \text{(Formula 8)}$$

It is well known that probabilities P_0 depend on manifestations of dangerous natural processes, on the condition of the critical infrastructure site, and consequently on P_T. Here the probability of terrorist impacts on special facilities in the technosphere (dams, mines, dangerous chemical storage facilities, mine tailing dumps at mining complexes) and on their operators and personnel also increases P_0.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

$$P_{OTR} = F_P\{(P_{NTR}),(P_{TTR})\} \quad \text{(Formula 9)}$$

Damages U_S from the realization of systemic threats can generally be written through the function F_{US}

$$U_S = F_{US}\{U_N, U_T, U_O\} \quad \text{(Formula 10)}$$

where U_N is the damages inflicted on the population by the interaction of primary and secondary impact factors in the realization of systemic threats, U_T is the damages inflicted on facilities in the technosphere, and U_O is the damages inflicted on the environment.

The magnitudes of U_N, U_T, and U_O may change in natural units (for example, by the number of people killed, the number of buildings destroyed, and the land area harmed) and in equivalents (for example, in economic and monetary indicators).

Terrorist acts are primarily manifested in increasing statistics regarding victims of the terrorist acts themselves U_{NTR}.

$$U_N = F_U\{(U_{NTR}),(U_{NO}, U_{NP}, U_{ND})\} \quad \text{(Formula 11)}$$

As noted earlier, with terrorist acts, damages to objects in the technosphere U_T and the natural environment U_O increase from manifestations of secondary and cascade impact factors.

$$U_T = F_U\{(U_{TTR}),(U_N)\} \quad \text{(Formula 12)}$$

$$U_O = F_U\{(U_{OTR}),(U_N, U_T)\} \quad \text{(Formula 13)}$$

In Russia, considering the socioeconomic transformations, the basic characteristics of the risks R of natural and technogenic accidents and catastrophes as defined by their severity T (or damages U) and numbers N (or probability P) are generally relatively complex in nature regarding their change over time t with an overall tendency toward increasing (see Figure 4).

The exceptional feature of the risks of terrorist incidents over the past 10 years is that the growth of the magnitude of the risks R, the probability of their occurrence P, and their damages U as measured in the number of victims is proceeding 5–10 times more intensively than the increase in the risks, probability, and damages for natural, natural-technogenic, and technogenic extreme situations.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

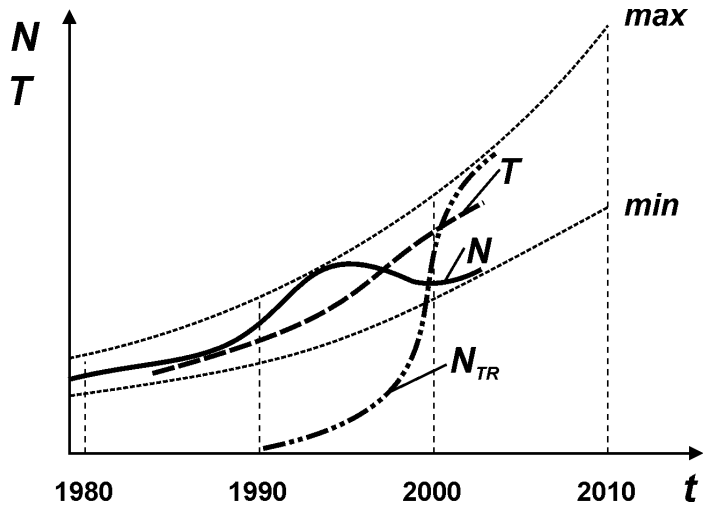


FIGURE 4 Change over time in the number N and severity T of catastrophes.

National, regional, and facility-level management, regulation, and security efforts according to systemic risk criteria R_s feeds into a qualitative and quantitative probabilistic, statistical, and deterministic analysis for the given time period Δt of all parameters in Formulas 1–13 and implementation of comprehensive measures to reduce systemic risks from the actual unacceptable levels R_S to acceptable (allowable) levels $[R_S]$:

$$R_S = P_S U_S \le \left(1/n_S\right) \cdot \left[R_S\right] = \left(1/n_S\right) \cdot \left[P_S\right] \cdot \left[U_S\right] = F_Z\left(m_Z Z\right) \qquad \text{(Formula 14)}$$

where n_s is the safety coefficient for systemic risks, $[P_S]$ and $[U_S]$ are the acceptable (allowable) probabilities and damages, Z is expenditures for risk reduction, and m_z is expenditure effectiveness ($1 \le m_z \le 10$).

Security according to the risk criteria R_S may be considered assured if the inequality $n_S \ge 1$ is achieved.

For Russia, based on fundamental risk indicators, the magnitudes of n_S are extremely low at present (no more than 0.1).

The time period Δt for which it is possible to determine risks R_S is generally taken at 1 year (Δt = 1 year).

In accordance with Formula 14, management of security and planning for its improvement using a risk-based set of criteria leads to the following primary tasks:

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

- developing scientific methods for analyzing risks R_S and their basic parameters P_S and U_S according to the system comprised by Formulas 1–6 and 10
- deciding on the level of acceptable magnitudes $[R_s]$, $[P_s]$, and$[U_s]$ while assessing the magnitudes of reserve resources n_s
- making a scientifically based determination of the level of expenditures Z for risk reduction while selecting and increasing the effectiveness of these expenditures (m_z)

In managing the risk of terrorism R_{STR} according to Formula 14, the characteristics U_{NTR}, P_{NTR}, U_{TTR}, P_{TTR}, U_{OTR}, and P_{OTR} must first be singled out and determined according to Formulas 7–9 and 11–13. These characteristics necessitate separating out the component Z_{TR} for the reduction of risks R_{STR} along with its expenditure effectiveness m_{ZTR} from overall risk reduction expenditures Z.

Here, predicting, monitoring, and preventing accidents and catastrophes at critical facilities turn out to be substantially more efficient than eliminating the consequences of emergency situations. With the appropriate foundations for risk reduction measures, the magnitudes Z can be significantly lower (m_z times) than the damages U_{STR} inflicted on the economy by the unprotectedness of critical facilities against terrorist acts.

In developing the fundamentals of state policy, the regulatory and legal base, draft plans for federal programs and pilot industry-wide and facility-wide projects to protect critical facilities, the population, and the vital infrastructure against threats of a technogenic, natural, and terrorist nature, the following areas of scientific research and development have the greatest significance:

- developing a base of scientific criteria for assessing the status of critical facilities and preparing a state registry of such facilities appropriate for protection against terrorist actions
- creating scientific foundations and principles for the design, construction, and operation of facilities and building systems for their protection
- creating theories and methods for control, diagnostics, monitoring, and forecasting of terrorism risks for critical facilities, operators, and personnel at the stages of their design, construction, operation, and removal from service
- developing educational and methodological foundations for training and retraining specialists and managers at all levels in ensuring protection for critical facilities and analyzing and managing risks of terrorism

BUILDING A SYSTEM TO PROTECT AGAINST TERRORISM

Based on the experience of the atomic energy and missile/aerospace technology industries in analyzing extreme situations of a technogenic nature, including those initiated by terrorist acts, it has been proposed to classify accident situations according to the degree of protection against them. The various types

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

TABLE 2 Types of Accident Situations and Degrees of Protection

No.	Normal (regular) or accident situations	Analysis of the risk of technological terrorism	Degree of protection against accidents and catastrophes
1	Normal conditions	Not conducted	Heightened
2	Deviations from normal conditions	Not mandatory	Sufficient
3	Design-related accidents	Mandatory	Partial
4	Not designed accidents	Necessary	Insufficient
5	Hypothetical accidents	Important	Low

of accidents and catastrophic situations in the technogenic sphere may be represented as follows (see Table 2) according to their degree and likelihood of occurrence at potentially dangerous facilities:

- operational—under normal operating conditions, occur during staff operation of potentially dangerous facilities; have predictable consequences; high degree of protection against them
- design-related—occur when ordinary operating regimes are exceeded; have predictable and acceptable consequences; sufficient protection against them
- not designed—occur as a result of irreversible damages to key components with heavy damages and high numbers of casualties; insufficient degree of protection against them; require subsequent reconstruction work at the facility
- hypothetical—can occur as a result of previously unforeseeable scenarios of development and entail the maximum possible damages and casualties; low degree of protection against them; direct restoration of facilities impossible

Whereas until recently it was believed that major acts of terrorism could primarily create hypothetical accident situations, now in a number of cases analysis of the risks of terrorism must be extended to not designed and design-related accidents as well. This entails a need to analyze the initiating actions of the primary, secondary, and cascade impact factors and the degree of protection against them at all stages of design, construction, and operations of potentially dangerous facilities.

In developing methods and systems for protecting against technological terrorism, the two basic tasks listed below must be taken into account:

1. reducing the risks of initiating actions
2. reducing the risks of extreme situations initiated by terrorist acts

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

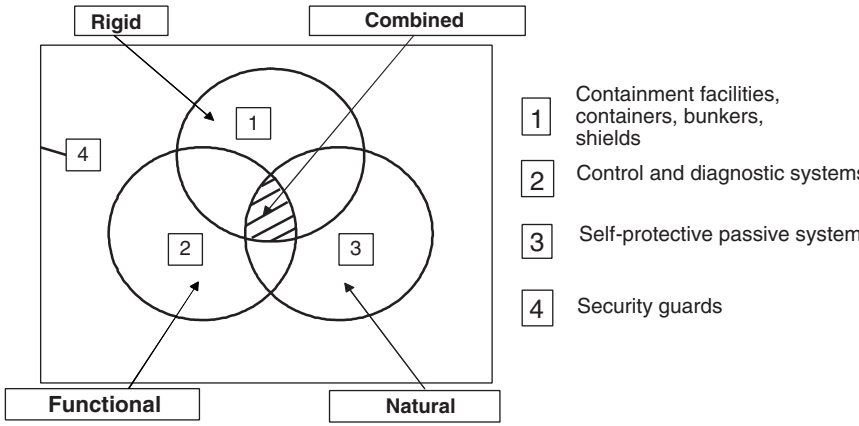


FIGURE 5 Types and systems of protection against accidents and catastrophes.

To protect elements of the engineered environment from terrorist-initiated actions and consequent extreme situations, the following types of protection systems are being studied and developed (see Figure 5):

- rigid protection—protection requiring the expenditure of a large amount of energy to overcome
- continuous functional protection—protection that in an accident or deviation from normal operational status for the elements of a complex technical system could take on certain system functions for a limited time or could prevent an accident from progressing further
- natural protection—protection that involves the use of passive natural phenomena and processes aimed at curtailing accidents and reducing the level of impact factors
- security guards

Circles 1, 2, and 3 stand for separate types of protection systems. Areas of intersection (1-2, 2-3, 1-3, and 1-2-3 correspond to a combination of correspondent types of protection systems. Security guards system 4 is organized to ensure protection of all the systems (1, 2, 3, 1-2, 2-3, 1-3, and 1-2-3).

Here the degree of protection against accident situations by all methods remains varied (see Table 2).

Regarding the problem of technological terrorism, in addition to the protection systems mentioned above there is also a specialized security protection system covering very high risk facilities, their personnel, and existing physical protective barriers. These security forces include the appropriate militarized and

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

specialized subunits equipped with weapons and military hardware and observation and warning systems. Combined protection unites the properties of intensive, functional, natural, and security personnel-based protection systems.

One of the most important factors in overcoming all of the types of terrorism discussed in this paper has been and remains that of direct counteractions against those who organize and carry out terrorist acts.

ADDITIONAL REFERENCES

General Council of the Russian Federation Scientific Research Institute of Problems of Reinforcing Law and Order. 2002. P. 134 in Terrorism and Transportation Security: A Compilation of Materials from an International Scientific and Practical Conference. Moscow: NII GP.

Makhutov, N. A., V. Osipov, and M. Gadenin. 2002. Scientific Basis for Ensuring Comprehensive Safety of Russia. Problems of Safety and Emergency Situations 6:13–21.

Makhutov, N. A., M. Segal, and V. Stepanchikov. 2004. Threats of Terrorism and Engineered Emergencies. Problems of Safety and Emergency Situations 2:85–93.

National Research Council. 2004. Pp. 227–228 in Terrorism—Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings. Washington, D.C.: The National Academies Press.

Russian Academy of Sciences-Russian Ministry of Emergency Situations. 2004. P. 313 in Problems of Technological Terrorism and Methods of Countering Terrorist Threats: A Compilation of Materials from a Scientific and Practical Conference. Moscow: Institute of Mechanical Engineering of the Russian Academy of Sciences.

Starostin, S. A. 2003. Modern Terrorism—a Threat to the National Security of the Russian Federation. Problems of Security in Extreme Situations 4:76–83.

Vorobiev, Yu., N. A. Makhutov, and G. Malinetky. 1998. Risk Theory and Technologies for Ensuring Safety: An Approach Based on Nonlinear Science. Problems of Safety and Emergency Situations 11:5–21.

Zmeevsky, A. V. 2002. Terrorism in a High-Tech Society: Legal Aspects and Conemporary Methods of Preventing and Countering Terroist Activity. P. 244 in High-Impact Terrorism: Proceedings of a Russian-American Workshop. Washington, D.C.: National Academy Press.

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

Appendixes

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

Appendix A

Agenda and List of Participants

U.S.-Russian Challenges in Countering Urban Terrorism
January 27–February 4, 2005

Thursday, January 27, 2005

8:30 *Breakfast*

9:00 Opening remarks for three working groups, discussion of working group objectives
George Bugliarello, Polytechnic University

9:30 Discussion of report format
Glenn E. Schweitzer, National Research Council

10:00 *Break*

Working Group on Energy Vulnerabilities

10:15 Discussion of task

10:30 Briefing on the East Coast power failure (2003)
U.S. Department of Energy

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

11:30 Presentation on upcoming study on Enhancing the Robustness and Resilience of Future Electric Transmission and Distribution in the United States to Terrorist Attack
James J. Zucchetto, Division on Engineering and Physical Sciences, National Research Council

12:30 *Working Lunch*

1:30 Presentations on Energy Issues
Aleksandr Yu. Kudrin, Main Administration for the City of Moscow of the Russian Ministry of Emergency Situations; Center for Monitoring and Forecasting of Emergency Situations
Sergey G. Vasin, Department of Security and Counterterrorism, Ministry of Industry and Energy

3:00 Briefing by industry representatives from Edison Electric Institute

5:30 *Adjourn*

Friday, January 28, 2005

9:00 Briefings by specialists from the Association of Oil Pipelines

10:30 Briefings by industry representatives at the National Petroleum Institute

1:30 Aleksandr Yu. Kudrin and Sergey G. Vasin join Working Group on Transportation Vulnerabilities for site visit to CHART facility

Working Group on Energy Vulnerabilities

Co-chair: Aleksandr Yu. Kudrin, Main Administration for the City of Moscow of the Russian Ministry of Emergency Situations; Center for Monitoring and Forecasting of Emergency Situations
Co-chair: Edward V. Badolato, The Shaw Group
Sergey G. Vasin, Department of Security and Counterterrorism, Ministry of Industry and Energy
Benjamin S. Cooper, Association of Oil Pipelines
Staff: Glenn E. Schweitzer, National Research Council

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Working Group on Transportation Vulnerabilities

Thursday, January 27, 2005

10:15 Presentation on relevant activities of the National Academies
Stephan Parker, Transportation Research Board, National Research Council

11:00 Presentation on relevant Russian Academy of Sciences activities
Nikolay A. Makhutov, Institute of Mechanical Engineering of the Russian Academy of Sciences

12:00 *Lunch*

1:00 Review of report format and draft
Mortimer L. Downey, PB Consult

1:30 Discussion of draft

2:00 *Break*

2:15 Presentation by Michael C. Smith, SAIC and University of Virginia

3:00 Visit to Washington Metropolitan Area Transit Authority Headquarters

Friday, January 28, 2005

9:00 Preparation of working group's report and slides

10:00 Presentation by Robert E. Gallamore, Transportation Center, Northwestern University

12:30 *Lunch*

1:30 Departure for Maryland State CHART Facility, Hanover, MD

Working Group on Transportation Vulnerabilities

Co-chair: Mortimer L. Downey, PB Consult
Co-chair: Nikolay A. Makhutov, Institute of Mechanical Engineering of the Russian Academy of Sciences
George W. Burns, III, Washington Metropolitan Area Transit Authority

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Robert E. Gallamore, Transportation Center, Northwestern University
Konstantin V. Frolov, Institute of Mechanical Engineering of the Russian Academy of Sciences
Staff: Kelly Robbins, National Research Council

Working Group on Cyberterrorism Issues

Thursday, January 27, 2005

10:15 Presentation on relevant activities at the National Academies
Herbert S. Lin, Division on Engineering and Physical Sciences, National Research Council

11:00 Presentation on relevant activities in Russia
Igor Fedorov and Nikolay V. Medvedev, Bauman Moscow State Technical University

12:00 *Lunch*

1:00 Depart for DHS visit

1:30 DHS Cyber Security Division site visit
Nohemi Zerbi, U.S. Department of Homeland Security
Liesyl Franz, U.S. Department of Homeland Security
Erica Russell, U.S. Department of State

3:00 Review of Conference on Grand Challenges in Information Security and Assurance, November 16–19, 2003
Anita K. Jones, University of Virginia

3:45 *Break*

4:00 Review of report format and draft to date
Anita K. Jones, University of Virginia

4:30 Discussion of draft

5:30 *Adjourn*

Friday, January 28, 2005

9:00 Cyber Issues at CERT, conference call
Casey Dunlevy, CERT

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

9:40 Depart for D.C. Emergency Operations Center, 2000 14th Street, NW, 8th Floor

10:00 D.C. Emergency Management Agency visit
Barbara Childs-Pair, D.C. Emergency Management Agency
Ned Ingraham, D.C. Emergency Management Agency

12:30 *Lunch*

1:30 Completion of report and presentation slides

3:00 *Break*

3:15 Completion of report and presentation slides

5:30 *Adjourn*

Working Group on Cyberterrorism Issues

Co-chair: Anita K. Jones, University of Virginia
Co-chair: Igor Fedorov, Bauman Moscow State Technical University
Lewis M. Branscomb, John F. Kennedy School of Government, Harvard University
Nikolay V. Medvedev, Department of Information Security, Bauman Moscow State Technical University
Yury K. Shiyan, Presidium of the Russian Academy of Sciences
Linton Wells III, University of Virginia
Michael Wolin, University of Virginia
Staff: A. Chelsea Sharber, National Research Council

Workshop on U.S.-Russian Challenges in Countering Urban Terrorism
Plenary Sessions

Monday, January 31, 2005

Session 1: Working Group and Participant Reports on Urban Terrorism
Chairs: Siegfried S. Hecker, Nikolay Platé

8:00 *Breakfast*

8:30 Opening Remarks: Agenda, Anticipated Outcome, and Content of Workshop Report

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

9:00 Report of Energy Vulnerabilities Working Group

9:30 Report of Transportation Vulnerabilities Working Group

10:00 Report of Cyberterrorism Issues Working Group

10:30 Discussion of Working Group Activities

11:00 *Break*

11:15 News and Terrorism: Communicating in a Crisis
Randy Atkins, National Academy of Engineering

11:45 Overview on Urban Terrorism in Russia
Konstantin V. Frolov, Institute of Mechanical Engineering of the Russian Academy of Sciences

12:15 Terrorist Acts in Moscow: Experience and Lessons in Eliminating Their Consequences
Aleksandr Yu. Kudrin, Main Administration for the City of Moscow of the Russian Ministry of Emergency Situations; Center for Monitoring and Forecasting of Emergency Situations

12:45 *Lunch*

Session 2: Discussion of Integration of Responses of Different Organization
Chairs: George Bugliarello, Konstantin V. Frolov

1:45 Introductory Remarks
Konstantin V. Frolov, Institute of Mechanical Engineering of the Russian Academy of Sciences

2:00 Overview of Integration of Responses of Different Organizations
George Bugliarello, Polytechnic University

2:15 Special Problems Posed by Fires
Nikolay P. Kopylov, Scientific Research Institute for Fire Prevention Defense of the Russian Ministry of Emergency Situations

2:45 A Decision Informatics Approach to Urban Emergency Management
James M. Tien, Rensselaer Polytechnic Institute

3:15 *Break*

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

3:30 Responsibilities of Russian Ministries When Responding to Incidents
Sergey G. Vasin, Department of Security and Counterterrorism, Ministry of Industry and Energy

4:00 Defending Against a Large City Attack: The Interdependence of Defense Strategies
Lewis M. Branscomb, Harvard University

4:30 General Discussion of Urban Terrorism

5:30 Signing of New Interacademy Agreement

6:00 *Adjourn*

Tuesday, February 1, 2005

Session 3: Review of U.S. and Russian Ongoing Projects Dealing with Terrorism
Chairs: Siegfried S. Hecker, Leonid Bolshov

8:30 Terrorism Studies of the National Academies
Wm. A. Wulf, National Academy of Engineering

9:15 Terrorism-related Activities of the RAS
Nikolay Platé, Russian Academy of Sciences

10:00 Report on Project on Conflict and Reconstruction in Multiethnic Societies
Robert McC. Adams, University of California at San Diego
Valery Tishkov, Institute of Ethnology and Anthropology of the Russian Academy of Sciences

10:30 *Break*

10:45 Report on Project on U.S.-Russian Cooperation in Combating Radiological Terrorism
Ionizing Radiation Sources
Leonid Bolshov, Nuclear Safety Institute of the Russian Academy of Sciences
Other Dimensions of Radiological Terrorism
John F. Ahearne, Sigma Xi, the Scientific Research Society

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

11:15 Biological Terrorism—Regional Emergency Preparedness
Russ Zajtchuk, Chicago Hospitals International

11:30 General Discussion of Presentations

12:00 *Lunch*

Session 4: Practical Perspectives on Recent Events Related to Terrorism and Terrorist Acts
Chairs: Siegfried S. Hecker, Leonid Bolshov

1:00 Lessons from Beslan, Russia
Gennady Kovalenko, Presidum of the Russian Academy of Sciences

1:45 A Discussion on Science and Technology Interests of the U.S. Department of Homeland Security
Brooke Buddemeier, U.S. Department of Homeland Security

2:15 U.S. Department of Homeland Security Science Advisory Committee
Ronald Taylor, U.S. Department of Homeland Security

2:45 Role of National Laboratories in Supporting Counterterrorism
Donald Prosnitz, Lawrence Livermore National Laboratory

3:15 U.S. Antiterror Policy and the 9/11 Commission Report
Raphael Perl, Congressional Research Service

3:45 *Break*

4:00 Role of the National Security Council of the Russian Federation in Countering Terrorism
Valentin A. Sobolev, National Security Council of the Russian Federation

4:30 Major Issues in Chemical and Biological Terrorism
Michael Moodie, Chemical and Biological Arms Control Institute

5:00 Cybercrime and the Training of Cybercrime Prevention Specialists in Russia
Nikolay V. Medvedev, Bauman Moscow State Technical University

6:00 Risk Assessment Methodologies for Terrorism
Nikolay A. Makhutov, Institute of Mechanical Engineering of the Russian Academy of Sciences

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

6:30 *Adjourn*

Wednesday, February 2, 2005

Session 5: Next Steps in Interacademy Cooperation in the Field of Counterterrorism
Chairs: Siegfried S. Hecker, Nikolay Platé

8:30 Current Organizational Issues Within the RAS
Nikolay Platé, Russian Academy of Sciences

9:30 Update on the International Visitors Office
Wendy White, Policy and Global Affairs, National Research Council

9:45 Discussion of Next Steps in Interacademy Cooperation in the Field of Counterterrorism

12:00 Visit to the National Academy of Sciences Marian Koshland Science Museum

Site Visits and Presentations in New York City
Arranged by Polytechnic University

Thursday, February 3, 2005

9:00 Ground Zero Presentation
General Introduction
George Bugliarello, Polytechnic University

Ground Zero Overview
George J. Tamaro, Mueser Rutledge Consulting Engineers

10:45 Visit to Ground Zero
Peter Rinaldi, Port Authority of New York and New Jersey

12:00 *Lunch*

1:00 Presentation on Metrotech
George Bugliarello, Polytechnic University

1:15 Sensors and Sensor Networks
Kalle Levon, Research and Intellectual Property, Polytechnic University

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

2:00 Emergency Response
William A. Wallace, Decision Sciences and Engineering Systems, Rensselaer Polytechnic Institute

2:45 *Break*

3:15 New York City Office of Emergency Management
Joseph F. Bruno, Commissioner
Sam Benson, Director of Health and Medical Preparedness

Friday, February 4, 2005

9:00 Presentation at the Traffic Management Center
Inspector Patrick J. McCarthy, Commanding Officer, Traffic Management Center, New York City Police Department
Lt. Joe Wolff, Traffic Management Center, New York City Police Department

11:00 *Break*

11:15 Intelligent Transportation Systems
Raman Patel, Urban Intelligent Transportation Systems Center, Polytechnic University

12:00 *Lunch*

1:00 Cybersecurity
Nasir Memon, Information Systems and Internet Security Laboratory, Polytechnic University

2:00 Long Island Electric Power Supply: Securing the System, Presentation at KeySpan
Edward J. Youngling, Electric Transmission and Distribution, KeySpan

Participants in the Workshop on U.S.-Russian Challenges in Countering Urban Terrorism and the Site Visits and Presentations in New York City

Participants on the National Research Council Committee on Counterterrorism Challenges for Russia and the United States

Robert McC. Adams, Adjunct Professor, University of California at San Diego

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

John F. Ahearne, Director, Ethics Program, Sigma Xi, The Scientific Research Society
Lewis M. Branscomb, Aetna Professor of Public Policy and Corporate Management, Emeritus, John F. Kennedy School of Government, Harvard University
George Bugliarello, President Emeritus and University Professor, Polytechnic University
Siegfried S. Hecker, Director Emeritus, Los Alamos National Laboratory; Visiting Professor, Center for International Security and Cooperation, Stanford University
Anita K. Jones, Lawrence R. Quarles Professor of Engineering and Applied Science, University of Virginia
Michael Moodie, Independent Consultant and Former President, Chemical and Biological Arms Control Institute
Wm. A. Wulf, President, National Academy of Engineering, *Ex-officio*
Russ Zajtchuk, President, Chicago Hospitals International

Participants from Russia

Ivan I. Belyaev, Deputy Director, Department for State Policy in Science, Innovation Activities, and Intellectual Property Rights, Ministry of Education and Science
Leonid Bolshov, Director, Nuclear Safety Institute of the Russian Academy of Sciences
Igor Fedorov, Rector, Bauman Moscow State Technical University
Konstantin V. Frolov, Director, Institute of Mechanical Engineering of the Russian Academy of Sciences
Nikolay P. Kopylov, Director, Scientific and Research Institute for Fire Prevention Defense of the Russian Ministry of Emergency Situations
Gennady Kovalenko, Presidium of the Russian Academy of Sciences
Aleksandr Yu. Kudrin, Deputy Director, Main Administration for the City of Moscow of the Russian Ministry of Emergency Situations; Director, Center for Monitoring and Forecasting of Emergency Situations
Nikolay A. Makhutov, Head of Department, Institute of Mechanical Engineering of the Russian Academy of Sciences
Nikolay V. Medvedev, Chair, Department of Information Security, Bauman Moscow State Technical University
Nikolay Platé, Vice President, Russian Academy of Sciences
Yury K. Shiyan, Chief Expert, Head of the Desk on Cooperation with North and Latin American Countries, Foreign Relations Department, Presidium of the Russian Academy of Sciences
Valentin A. Sobolev, Deputy Chair, National Security Council of the Russian Federation

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Valery Tishkov, Director, Institute of Ethnology and Anthropology of the Russian Academy of Sciences
Sergey G. Vasin, Deputy Director, Department of Security and Counterterrorism, Ministry of Industry and Energy

Participants in Washington, D.C.

Randy Atkins, Senior Program Officer, National Academy of Engineering
Edward V. Badolato, Executive Vice President of Homeland Security, The Shaw Group
Brooke Buddemeier, Science and Technology, U.S. Department of Homeland Security
George W. Burns III, Counterterroism Coordinator, WMD, Metro Transit Police Department, Washington Metropolitan Area Transit Authority
Barbara Childs-Pair, Director, D.C. Emergency Management Agency
Benjamin S. Cooper, Executive Director, Association of Oil Pipe Lines
Mortimer L. Downey, Chairman of the Board, PB Consult
Casey Dunlevy, Senior Member of the Technical Staff, CERT
Liesyl Franz, Public Policy and International Affairs, National Cyber Security Division, U.S. Department of Homeland Security
Robert E. Gallamore, Professor of Managerial Economics and Decision Sciences, Kellogg School of Management, Transportation Center, Northwestern University
Christopher Holt, Senior Program Assistant, Policy and Global Affairs, National Research Council
Ned Ingraham, D.C. Emergency Management Agency
Herbert S. Lin, Senior Scientist, Division on Engineering and Physical Science, National Research Council
Stephan Parker, Senior Program Officer, Transportation Research Board, National Research Council
Raphael Perl, Specialist in International Affairs, Congressional Research Service
Donald Prosnitz, Deputy Director, Homeland Security Organization, Lawrence Livermore National Laboratory
Kelly Robbins, Senior Program Officer, Policy and Global Affairs, National Research Council
Erica Russell, Office of Plans, Policy, and Analysis, U.S. Department of State
Glenn E. Schweitzer, Program Director, Policy and Global Affairs, National Research Council
A. Chelsea Sharber, Senior Program Associate, Policy and Global Affairs, National Research Council
Michael C. Smith, SAIC, and Associate Professor of Systems and Information Engineering, University of Virginia

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

Ronald Taylor, Director, Office of Studies and Analysis, Science and Technology, U.S. Department of Homeland Security
James M. Tien, Chair and Professor of Decision Sciences and Engineering Systems, School of Engineering, Rensselaer Polytechnic Institute
Linton Wells III, University of Virginia
Wendy White, Director, BISO, Policy and Global Affairs, National Research Council
Michael Wolin, University of Virginia
Nohemi Zerbi, International Branch, Strategic Partnerships Office, Information Analysis and Infrastructure Protection, U.S. Department of Homeland Security
James J. Zucchetto, Director, BEES, Division on Engineering and Physical Sciences, National Research Council

Participants in New York City

Sam Benson, Director of Health and Medical Preparedness, New York City Office of Emergency Management
Joseph F. Bruno, Commissioner, New York City Office of Emergency Management
Seth Cummins, Chief of Staff, New York City Office of Emergency Management
Stuart Klein, Associate Director, Urban Security Initiative, Polytechnic University
Kalle Levon, Research and Intellectual Property, Polytechnic University
Patrick J. McCarthy, Commanding Officer, Traffic Management Center, New York City Police Department
Nasir Memon, Information Systems and Internet Security Laboratory, Polytechnic University
Raman Patel, Urban Intelligent Transportation Systems Center, Polytechnic University
Peter Rinaldi, General Manager, World Trade Center Priority Capital Programs, Port Authority of New York and New Jersey
George J. Tamaro, Partner, Mueser Rutledge Consulting Engineers
William A. Wallace, Decision Sciences and Engineering Systems, Rensselaer Polytechnic Institute
Joseph Wolff, ITS Coordinator, Traffic Management Center, New York City Police Department
Edward J. Youngling, Vice President, Electric Transmission and Distribution, KeySpan

Copyright National Academy of Sciences. All rights reserved.

Appendix B

Russian Academy of Sciences-U.S. National Academies Joint Committees on Countering Terrorism

Glenn E. Schweitzer
National Research Council

Since 2001, three collaborative workshops on counterterrorism have been held by the Russian Academy of Sciences and the U.S. National Academies. Joint committees on countering terrorism were established by the Russian Academy of Sciences and the U.S. National Academies in 2002.[1] The first workshop was convened in June 2001 in Moscow, and presentations covered a wide range of terrorist threats and vulnerabilities to those threats. *High-Impact Terrorism: Proceedings of a Russian-American Workshop* was published in English and Russian in 2002. The second workshop was organized in March 2003 in Moscow with an emphasis on urban terrorism and cyberterrorism. *Terrorism—Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings* was published in English and Russian in 2004. The third workshop was held in January–February 2005 in Washington, D.C., and proceedings are scheduled for publication in English and Russian.

Building on the work of the first two workshops, the joint committees selected the theme of urban terrorism for the third workshop. Working groups on energy vulnerabilities, transportation vulnerabilities, and cyberterrorism issues convened prior to the workshop, and each panel reported its findings at the workshop. A special workshop session was then devoted to the challenges in coordinating activities of the many governmental and nongovernmental organizations that would be involved in responding to a terrorist attack in an urban area. Discussions of other special interest topics followed.

[1]For more information about the U.S. National Academies work in cooperation with the Russian Academy of Sciences on counterterrorism, see http://www7.nationalacademies.org/dsc/CT_Project.html.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

During the sessions of the working panels and then following the workshop, the Russian visitors met a number of additional U.S. specialists involved in the topics that were discussed. Also they visited relevant facilities and met with first responders in Washington, D.C.; Hanover, Maryland; and New York City.

Returning to the second workshop, held in 2003, the joint committees established five standing working groups to assist the committees in addressing a broad range of issues. The status of these working groups is summarized below.

WORKING GROUP ON RADIOLOGICAL TERRORISM

At each of the three workshops, presentations highlighted the dangers associated with radiological terrorism. They described a variety of attack scenarios and emphasized that the psychological impact of the dispersion of radioactivity might far exceed the physical harm from radiation exposure. As a result of the discussions at the workshops, the U.S. National Academies, with the assistance of the Russian Academy of Sciences and in consultation with many Russian specialists, is undertaking a study of the current cooperative program between the U.S. Department of Energy (DOE) and the Russian Federal Agency for Atomic Energy (Rosatom). The Institute of Nuclear Safety of the Russian Academy of Sciences is playing a particularly active role in this effort.

The emphasis of the intergovernmental cooperative program has been on reducing the possibility that ionizing radiation sources in Russia could fall into the hands of terrorists. A special workshop was held in Moscow in March 2005 to consider the current status of security over ionizing radiation sources, and the Russian Institute for Nuclear Safety prepared an overview of the current approach to improving security in Russia. The final report for this activity will be published by the National Academies Press.

WORKING GROUP ON BIOLOGICAL TERRORISM

The National Academies have had a long-standing program, carried out in its initial phase with the assistance of the Russian Academy of Sciences, for promoting the redirection to civilian tasks of Russian scientists who previously carried out research in support of the Soviet defense complex. Initially the program was considered a nonproliferation activity to prevent unreliable states from gaining access to information about biological weapons. However, as international terrorists increase their technical capabilities, the relevance of the program to the terrorism interests of the joint committees is clear.

Related to this activity has been a study by the National Academies that considers the future of biosciences and biotechnology in Russia. It emphasized the importance of public health concerns, focusing on disease surveillance, biological research, the evolution of the biotechnology industry, zoonotic diseases, and the strengthening of the science and technology workforce, with opportuni-

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

ties for international cooperation overarching each of these areas. The study was carried out with the assistance of the Russian Academy of Sciences and involved intensive consultations by the U.S. specialists responsible for the study with a number of Russian officials and scientists. The report of the study was published in English and Russian in 2006.[2]

WORKING GROUP ON URBAN TERRORISM

As discussed above, urban terrorism has received continuing attention by the joint committees, and the working group played a major role in organizing the third workshop. Many papers have been prepared by Russian and U.S. program participants on various aspects of urban terrorism, and a number of these papers will be included in the proceedings of the third workshop. Russian presentations have addressed several terrorist incidents in Moscow and other Russian cities, including the seizure of more than 900 hostages at a theater in Moscow, the bomb detonation in a crowded subway car in Moscow, and the seizure by terrorists of a school in Beslan that resulted in more than 300 deaths. U.S. presentations have addressed a number of aspects of the consequences of the September 11, 2001, attacks on the World Trade Center.

As to future steps, the fourth workshop of the joint committees may be held in Moscow and may also be devoted to urban terrorism. It seems appropriate to include a significant number of first responders from both countries in future discussions of urban terrorism.

WORKING GROUP ON CYBERTERRORISM

Cyberterrorism has been on the agenda of all three workshops. The disruptive effects of cyberterrorism targeted at critical communication lines or control facilities continue to be of great concern in both countries. Should cyberterrorism be directed to emergency response networks at the time of an attack using conventional explosives in an urban area, the consequences could be significant.

Specialists from both countries have shown great interest in the development of higher education curricula devoted to preparing specialists in cybersecurity. The program at the Bauman Moscow State Technical University has been considered very impressive by all participants. Consideration is being given to arranging a short course in Moscow for U.S. students, but the details have yet to be worked out.

---

[2]NRC Committee on Future Contributions of the Biosciences to Public Health, Agriculture, Basic Research, Counter-terrorism, and Non-Proliferation Activities in Russia. 2006. Biological Science and Biotechnology in Russia: Controlling Diseases and Enhancing Security. Washington, D.C.: The National Academies Press.

Copyright National Academy of Sciences. All rights reserved.

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop

WORKING GROUP ON THE ROOTS OF TERRORISM

This working group has been active for several years, and its efforts were linked to the work of the joint committees in 2001. The initial activities of the working group concentrated on ethnicity-related issues in Russia, and particularly in the North Caucasus region. A number of workshops were held and several reports were prepared in English and Russian.

Now the activities of this group are being expanded to address the broader topic of roots and routes of extremism, with a broader geographical focus as well. A workshop was held in October 2005 in Helsinki, with participants including approximately 30 scholars and practitioners from the United States, Russia, Finland, other European countries, the Middle East, and Central Asia. Developments in countries with large Muslim populations were a primary focus of discussions, but the program also included presentations on extremism-related developments in Europe and the United States.

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.