





Russian Views on Countering Terrorism During Eight Years of Dialogue: Extracts from Proceedings of Four Workshops

ISBN
978-0-309-13757-7

362 pages
6 x 9
PAPERBACK (2009)

Glenn Schweitzer and Merc Fox, Editors; Office for Central Europe and Eurasia Development, Security, and Cooperation; Policy and Global Affairs; National Research Council; In cooperation with the Russian Academy of Sciences

 Add book to cart

 Find similar titles

 Share this PDF



Visit the National Academies Press online and register for...

- ✓ Instant access to free PDF downloads of titles from the
 - NATIONAL ACADEMY OF SCIENCES
 - NATIONAL ACADEMY OF ENGINEERING
 - INSTITUTE OF MEDICINE
 - NATIONAL RESEARCH COUNCIL
- ✓ 10% off print titles
- ✓ Custom notification of new releases in your field of interest
- ✓ Special offers and discounts

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

Russian Views on Countering Terrorism During Eight Years of Dialogue

Extracts from Proceedings of Four U.S.-Russian Workshops

Glenn Schweitzer and Merc Fox, *Editors*

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

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.

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 13: 978-0-309-13757-7

International Standard Book Number 10: 0-309-13757-8

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) 334-2376.

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 2009 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America.

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

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

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

www.national-academies.org

Preface

In June 1999, the presidents of the National Academy of Sciences (NAS) and the Russian Academy of Sciences agreed that a joint project on combating especially dangerous crimes, particularly terrorism, would be of considerable interest to both Russian and American specialists in a variety of fields. The president of the NAS requested the president of the National Academy of Engineering to assume responsibility for developing and implementing the project. Representatives of the Institute of Medicine became involved in the project shortly thereafter.

During the eight years that followed, several inter-academy planning meetings and four inter-academy workshops were held on various aspects of countering terrorism. The workshops were carried out under the leadership of Siegfried Hecker of Stanford University and Yevgeny Velikhov of Kuzchatov Institute of Atomic Energy. Site visits to relevant Russian government offices and facilities involved in countering terrorism followed each of the workshops. The Carnegie Corporation of New York provided generous financial support for these activities. Proceedings of the workshops have been published as follows:

High Impact Terrorism: Proceedings of a Russian-American Workshop, June 2001, National Academy Press, 2002

Terrorism—Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings, March 2003, The National Academies Press, 2004

Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop, January 2005, The National Academies Press, 2006

Countering Terrorism—Biological Agents, Transportation Networks, and Energy Systems: Summary of a U.S.-Russian Workshop, March 2007, The National Academies Press, 2009

This volume is a compilation of a number of the Russian papers included in the aforementioned proceedings. It should be of interest to U.S. specialists as well as to specialists from other countries who are working in the field of counter-terrorism, but who may not have ready access to the information that is presented. As demonstrated in the papers, Russia has been and should continue to be an important participant in global efforts to combat terrorism domestically and internationally.

The papers are organized according to the workshops where they were presented. The proceedings for each of the workshops contain additional Russian papers, all of the American papers, and reports of working groups, and can be found online at www.nap.edu.

Glenn Schweitzer, Director
Office for Central Europe and Eurasia

Contents

**Papers from *High Impact Terrorism: Proceedings
of a Russian-American Workshop (2002)***

Cooperation Among Ministries of Internal Affairs of CIS Member States in the Fight Against Terrorism and Other Manifestations of Extremism <i>Igor L. Dimitrov</i>	3
Russian Legislation and the Struggle Against Terrorism <i>Mikhail P. Kireev</i>	9
Selected Technologies and Procedures Intended to Restrict Unauthorized Access to Explosives <i>Bronislav V. Matseevich</i>	19
Bioterrorism: A View from the Side <i>Oleg S. Morenkov</i>	23
Electromagnetic Terrorism <i>Yury V. Parfyonov</i>	31

Russian Legislation and the Fight Against Terrorism <i>Viktor E. Petrishchev</i>	35
Could Terrorists Produce Low-Yield Nuclear Weapons? <i>Stanislav Rodionov</i>	47
Problems of Biological Security in Agriculture <i>Georgy A. Safonov and Vladimir A. Gavrilov</i>	51
International Centers as a Basis for Controlling Infectious Disease and Countering Bioterrorism <i>Lev S. Sandakhchiev (Deceased), Sergey V. Netesov, and Raisa A. Martynyuk</i>	61
The Role of Internal Affairs Agencies in Efforts to Fight Terrorism Under High-Technology Conditions <i>Oleg A. Stepanov</i>	71
Papers from <i>Terrorism—Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings (2004)</i>	
Analysis of the Threats and Consequences of Terrorist Acts in Urban Settings: Outline of a Protection System <i>Vladimir Z. Dvorkin</i>	81
Lessons Learned from the <i>Nord-Ost</i> Terrorist Attack in Moscow from the Standpoint of Russian Security and Law Enforcement Agencies <i>Yevgeny A. Kolesnikov</i>	93
Technical Protection of Electronic Documents in Computer Systems <i>Valery A. Konyavsky</i>	103
International Aspects of Creating a State System for Countering the Illegal Circulation of Radioactive Materials in the Russian Federation <i>Vladimir M. Kutsenko</i>	115
Computer Security Training for Professional Specialists and Other Personnel Associated with Preventing and Responding to Computer Attacks <i>Anatoly A. Malyuk, Nikolai S. Pogozhin, and Aleksey I. Tolstoy</i>	119
Medical Aspects of Combating Acts of Bioterrorism <i>Gennady G. Onishchenko</i>	129

CONTENTS

ix

Certain Aspects Regarding the Development of Conditions Favorable to Cyberterrorism and the Main Areas of Cooperation in the Struggle Against It	133
<i>Igor A. Sokolov and Vladimir I. Budzko</i>	
The Role of the Russian Ministry of Internal Affairs in Combating Terrorism in Urban Conditions	141
<i>Sergey A. Starostin</i>	
The Role of the Russian Ministry of Emergency Situations and Executive Branch Agencies of the City of Moscow in Dealing with Emergency Situations Arising from Acts of Terrorism	153
<i>Aleksandr M. Yeliseev</i>	
Papers from <i>Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop (2006)</i>	
Unauthorized Use of Radiation Sources: Measures to Prevent Attacks and Mitigate Consequences	161
<i>Leonid Bolshov, Rafael Arutyunyan, Elena Melikhova, and Oleg Pavlovsky</i>	
Special Characteristics of Firefighting in Urban Areas	179
<i>Nikolay P. Kopylov</i>	
On the Events in Beslan	199
<i>Gennady Kovalenko</i>	
Terrorist Acts in Moscow: Experience and Lessons in Eliminating Their Consequences	215
<i>Aleksandr Yu. Kudrin</i>	
Methodology for Assessing the Risks of Terrorism	221
<i>Nikolay A. Makhutov</i>	
Cybercrime and the Training of Specialists to Combat It in Russia	237
<i>Nikolay V. Medvedev</i>	
On Efforts to Counter International Terrorism in the Russian Federation and Possible Areas of U.S.-Russian Cooperation in this Area	247
<i>Valentin A. Sobolev</i>	

Efforts of Russian Ministries in Implementing Measures to Prevent Acts of Terrorism <i>Sergey G. Vasin</i>	257
---	-----

Papers from *Countering Terrorism—Biological Agents, Transportation Networks, and Energy Systems: Summary of a U.S.-Russian Workshop (2009)*

Electromagnetic Terrorism: Threat to the Security of the State Infrastructure <i>Vladimir Ye. Fortov and Yury V. Parfyonov</i>	271
---	-----

Use of Predictive Modeling Packages for Effective Emergency Management <i>Nikolai P. Kopylov and Irek R. Khasanov</i>	275
--	-----

Organizational Measures and Decision Support Systems for Preventing and Responding to Terrorist Acts at Potentially Hazardous Facilities, on Transportation Systems, and in Locations Where Large Numbers of People Congregate <i>A. Yu. Kudrin, A. I. Zaporozhets, and S. A. Kachanov</i>	289
---	-----

International and National Priorities in Combating Terrorism in the Transportation Sector <i>Vladimir N. Lopatin</i>	297
---	-----

Characteristics of Technological Terrorism Scenarios and Impact Factors <i>Nikolai A. Makhutov, Vitaly P. Petrov, and Dmitry O. Reznikov</i>	305
---	-----

Emerging Viral Infections in the Asian Part of Russia <i>Sergei V. Netesov and Natalya A. Markovich</i>	323
--	-----

Activities of the Russian Federal Medical-Biological Agency Related to Radiation, Chemical, and Biological Security <i>Vladimir V. Romanov</i>	339
---	-----

The Problem of Oil and Natural Gas Pipeline Supply <i>Sergei G. Serebryakov</i>	343
--	-----

Papers from
High Impact Terrorism:
Proceedings of a Russian-American
Workshop
(2002)

Cooperation Among Ministries of Internal Affairs of CIS Member States in the Fight Against Terrorism and Other Manifestations of Extremism

*Igor L. Dimitrov**

Main Administration for Legal Work and External Affairs,
Russian Ministry of Internal Affairs

Having directly encountered the problems caused by the process of the breakup of the USSR, field personnel from internal affairs agencies and other law enforcement structures were the first to conclude that joint efforts and coordinated actions are required in the fight against crime, which recognizes no boundaries. Therefore, measures to create an organizational-legal basis for cooperation with colleagues from neighboring states were undertaken right at the interagency level.

As early as the first meeting of internal affairs ministers of the Commonwealth of Independent States (CIS) member countries, which took place in Almaty in April 1992, participants signed an Agreement on Cooperation among the internal affairs ministries of the various independent states in the fight against crime. This treaty outlined the commitments of the parties first to work jointly to combat gangsterism, terrorism, and international crime and second to create a coordinating body, the Conference of Internal Affairs Ministers (SMVD).

At the same time, because the conference could not function on a continual basis, the Office for the Coordination of the Fight Against Organized Crime and Other Dangerous Types of Crime on the Territory of CIS Participant-States (BK-BOP) was created on September 24, 1993. This action was taken on the initiative of the conference and on the basis of a resolution of the Council of CIS Heads of Government. This structure essentially became the working arm of the SMVD and began regularly coordinating all areas of the fight against crime, including crime of a terrorist nature. Thus, the organizational-legal foundations for interagency cooperation in this field were successfully created at that time.

* Translated from the Russian by Kelly Robbins.

The question of the need to intensify cooperation in the fight against terrorism given the situations developing in the Caucasus and Central Asia was first raised separately at the April 1996 regular meeting of the Council of Ministers of Internal Affairs of CIS Member States in Dushanbe. As a result of discussion of these problems, participants in the meeting adopted a resolution consisting of practically 30 points, which specifically stipulated the following:

- Identifying within each ministry an agency responsible for coordinating antiterrorist activities within the framework of the ministries of internal affairs, with the BKBOP to be informed of this selection as soon as possible;
- Ensuring the systematic exchange of operational and other information about uncovered or developing terrorist organizations and individuals inclined to commit terrorist acts or involved in the manufacture of explosive devices;
- Carrying out coordinated activities to work out plans of actions to be taken to prevent and suppress terrorist acts;
- Instituting measures to discover and suppress the channels by which illegal armed formations, organized crime societies, and individuals obtain money and other assistance used in the commission of terrorist acts;
- Carrying out in 1996-1997 a comprehensive inventory of rifles in the possession of enterprises, organizations, institutions, and citizens as well as a listing of locations where explosive materials are stored, with operational coverage to be ensured regarding these locations; and
- Developing a standard checklist for urgent actions to be taken by duty officers of internal affairs agencies when reacting to cases of terrorism.

It should be noted that a substantial amount of joint work was done in implementing the stipulations of this document, and the results of this work were summarized at the June 1998 meeting of the council in Tashkent.

The next notable step in the strengthening of cooperation in this sphere was the resolution "On Cooperation in the Struggle Against Crimes of an Extremist Nature Committed on Religious Grounds," which was adopted during the next regular SMVD meeting in Moscow in December 1998. This resolution calls for carrying out a whole series of specific joint activities in this regard.

The Kiev meeting of the council on October 1, 1999, saw the passage of the resolution "On Combating Terrorism on the Territory of CIS Member States" and the Appeal to Heads of State and Heads of Government of CIS Countries. The first document stipulated the establishment of a Provisional Anti-terrorist Center under the auspices of BKBOP, with the new center to be given the functions of coordinating the activities of internal affairs agencies in combating terrorism and other manifestations of extremism. This unit was soon in fact created. The second document specifically called for the Council of CIS Heads of State to take a top-priority look at the problems of combating international terrorism.

In Moscow on January 25, 2000, the leaders of the CIS countries reviewed

these questions and adopted a resolution that later served as the basis for the passage of the Program of CIS Member States to Combat International Terrorism and Other Manifestations of Extremism through 2003. The resolution also created the CIS Antiterrorist Center (a representative of SMVD was appointed first deputy director of the center). It should be emphasized that the same day saw the adoption of the Intergovernmental Program of Joint Measures to Fight Crime for 2000 through 2003, which was developed with our active participation. Among other elements, the program calls for carrying out targeted inter-agency operational-preventive activities and special operations to suppress acts of terrorism and other manifestations of extremism.

The Council of Ministers of Internal Affairs met for the next time in Moscow on March 10, 2000, with the meeting being devoted entirely to issues regarding the strengthening of cooperation in the antiterrorist sphere. At the meeting, participants passed the appropriate resolutions, in particular calling for the following:

- Preparation of a multilateral interagency agreement on fighting terrorism and other manifestations of extremism;
- The regular holding of coordinated operational search and prevention exercises, especially the special operations entitled "Border-Barrier";
- The holding of joint training exercises for special militia (police) units and internal affairs troops to work out coordinated actions in the struggle against acts of terrorism;
- The facilitation of close interaction in the development and contracted provision of special means, technology, and equipment for carrying out antiterrorist activity; and
- The exchange on the basis of mutual agreement of specialists to render consultative and other assistance in the fight against terrorism.

The next meeting of SMVD, which was held in Cholpon-Ata in September 2000, saw the signing of the Agreement on Cooperation Among Internal Affairs Ministers in the Fight Against Terrorism. Participants also adopted corresponding resolutions aimed primarily at the full and absolute implementation of the above-mentioned intergovernmental programs. A council plan for carrying out these programs was later prepared and approved, and implementation of the plan has already been discussed at the regular SMVD meeting held in Yerevan in June 2001 (the appropriate joint resolutions were also passed as a result of consideration of this question).

In noting the basic stages in the development of cooperation on the given issue among the internal affairs agencies of the CIS countries within the framework of such multilateral bodies as the SMVD and BKBOP, one should also mention the very important work being done by other organizations. These include the "Borzhomi Four" (the Conference of Internal Affairs Ministers of Az-

erbaijan, Armenia, Georgia, and Russia), the “Bishkek Group” (the Conference of Leaders of Law Enforcement Agencies and Intelligence Services from the “Shanghai Five” Countries), and the Conference of Internal Affairs Ministers of the Black Sea Economic Cooperation Organization member states, as well as activities being conducted through the International Criminal Police Organization (Interpol). The notable role played by bilateral coordinating institutes—for example joint boards—should also be mentioned.

At present, such Russian Internal Affairs Ministry boards have been created with the internal affairs ministries of Armenia, Belarus, Georgia, and Tajikistan. For instance, within the framework of the Russian-Belarusan Joint Board, a Program of Joint Measures to Combat Terrorism and Other Manifestations of Extremism for 2000-2001 has been approved and is being carried out successfully. The Russian-Armenian Board has a Plan for Joint Actions on Combating Terrorism and the Illegal Trade in Weapons, Ammunition, Explosive Substances, and Explosive Devices for 2000-2001.

In addition, another sort of coordinating institution, the conference of heads of internal affairs agencies of border districts, has recently been developed. In the fall of 2000, such conferences, including the participation of the relevant internal affairs ministers, were held for Russian and Ukrainian officials (in Donetsk) and Russian and Kazakhstani officials (in Novosibirsk). During the meetings, these conferences were given permanent operating status.

Therefore, a very solid organizational basis for cooperation has been created along with the necessary treaties and legal arrangements. At present, a significant number of multilateral and bilateral agreements are in effect in the anticrime sphere at the interstate, intergovernmental, and interagency levels, and this process is continuing.

The internal affairs agencies of the CIS countries are working actively on the investigation of criminal cases; on questions of extradition and the protection of social order; on the development of information systems and special means, technology, and equipment; and on the training and continuing education of personnel. A system has been put in place for the exchange of operational information. Comprehensive investigations are being conducted regarding organizations and individuals suspected of involvement in the activities of terrorist or other extremist formations and criminal groups and societies.

In cooperation with other military structures, prevention and search operations are regularly conducted, along with special operations to prevent, uncover, suppress, and reveal crimes. There are a multitude of examples, including most importantly such activities as “Border,” “Border-Barrier,” “Channel,” “Transit,” “Passenger,” and “Foreigner.”

Despite the fact that the development of interagency cooperation within the CIS framework regarding the struggle against terrorism and other manifestations of extremism is going well on the whole, work on the further intensification of joint efforts in this regard is actively continuing. This is connected primarily

with the fact that these extraterritorial phenomena, which do not recognize the boundaries of state or political systems, today represent an enormous problem and a real force capable of opposing state institutions and threatening national security. This has been shown by events occurring in the Caucasus and Central Asia.

Therefore, it is difficult to overestimate the role and significance of close international cooperation in this sphere on the whole, including within the framework of the Commonwealth of Independent States. On this basis, we must continue to move forward on the road to a new millennium free from the threat of international terrorism and other manifestations of extremism.

Russian Legislation and the Struggle Against Terrorism

*Mikhail P. Kireev**

Academy of the Ministry of Internal Affairs

Terrorism, terrorists, and terrorist activity—these concepts appear in the media practically every day, bringing horror and fear to the population and giving rise to unease and well-founded alarm for our present and our future.

Let us try to get an understanding of the position of Russian legislation in the manner in which Russian laws protect the citizen from crimes of a terrorist nature, crimes with terrorist aspects, and terrorism itself, from the criminal-legal standpoint.

Objectively speaking, terrorism represents a complex and multifaceted phenomenon, the subjects of which infringe in various ways on many legally protected common goods in the pursuit of the most varied goals. This naturally gives rise to difficulties in developing a universal understanding of just what terrorism means.

One of the most serious problems is that of defining the criminal-legal concept and correctly applying existing laws in the struggle against terrorism. A survey conducted among law enforcement agency personnel (more than 1000 individuals were polled) showed that 31 percent anticipate a stabilization in the level of terrorism, while another 31 percent expect a small rise and 13 percent forecast a significant rise. The data collected evoke concern, since the fundamental object of the struggle lies in relations of the security of civil society, characterized by stability and protection of those social conditions necessary for the normal activities of the population and the stable functioning of social institutions. At the same time, terrorism creates a threat not only to the security of society, but also to the security of the individual and to the lives and health of

* Translated from the Russian by Kelly Robbins.

people, as well as to the security of the state and the capacity of state institutions to fulfill their duties to society.

Of course, the question immediately arises as to the extent to which the actions of law enforcement agencies affect the stabilization of the situation. Among those polled, the overwhelming majority of 70 percent responded that these actions had a partial impact, 21 percent replied on the contrary that there was no such effect, and only 9 percent indicated that stabilization was entirely dependent on the actions of law enforcement.

The Criminal Code and the 1998 Federal Law on Combating Terrorism represent the key elements of Russian antiterrorism legislation. The Criminal Code of the Russian Federation defines actions that are considered to be terrorism or terrorist acts, including the differences between such actions and sabotage or other crimes. It also sets forth the punishments if such actions are committed. The code largely formulates the tasks of law enforcement agencies and intelligence services in uncovering, preventing, and suppressing terrorist activity and defining their goals, organizational structures, and means of using the results of preventive, antiterrorist, administrative, procedural, and other activities aimed at fighting terrorism.

The correct criminal-legal evaluation of information obtained by law enforcement agencies is highly significant in increasing the effectiveness and productivity of the struggle against terrorism. Evidence of this may be found in the results of our research. We shall point out the reasons, in our view, for the unsatisfactory state of the struggle against terrorism. Among the reasons most commonly cited, 24 percent of those surveyed blamed insufficient coordination and 18 percent pointed to a lack of decisiveness on the part of law enforcement officials during decision making.

On the whole, the 1996 Criminal Code of the Russian Federation regulates matters of responsibility for terrorism and terrorist acts in a new way. This is connected with certain changes and additions made in the texts of the corresponding articles of the Special Section of the code, other changes in many criminal-legal standards and institutions, and reforms in the state legal system of our country.

The criminal-legal concept of terrorism is set forth in Article 205 of the Russian Criminal Code. The objective aspect of this crime lies in the perpetration of bombings, arson, or other actions creating a danger of loss of life, significant property damage, or other socially dangerous consequences (an analysis of statistical data shows that 35 percent of terrorist acts involve bombings). The characterization in the new Criminal Code of certain possible consequences of terrorism as "socially dangerous" requires some limiting commentary.

Indeed, if the above-mentioned expression were interpreted literally, then any intentional crime committed in the aim of violating societal security would have to be viewed as an act of terrorism. After all, any crime is a socially dangerous action, that is, it entails or threatens to entail socially dangerous con-

sequences. Furthermore, in such a literal interpretation, the boundary would disappear between a deliberately false report of an act of terrorism (Article 207 of the Criminal Code) and a deliberately false report of a crime (deliberately false accusation) (Article 306). In the normative language on terrorism, the law has in mind not any dangerous consequences, but only those for which the danger is comparable to the danger of loss of life and significant property damage. In addition, the actions carried out must be capable of facilitating the achievement of terrorist goals as described in Article 205, that is, frightening the population, violating societal security, and influencing the decisions of organs of power. Therefore, the category of “other consequences” might include causing harm to the health of many people, making it impossible for the population to exercise its civil rights and freedoms, causing serious disruptions in the operation of vital services and organs of power, or leading to other such socially dangerous outcomes.

At the same time, the new Criminal Code is similar to previous legislation in that it does not require that the above-listed consequences actually occur in order for terrorism to be recognized as a committed crime. Moreover, even if in a case of bombing or arson, the real danger of loss of life, serious property damage, or other such consequences never actually arose due to measures taken, terrorism must be deemed as having been committed formally under Russian legislation.

The Criminal Code does not provide an exhaustive list of actions recognized as terrorism. It is supposed that these could include not only single one-time actions (arson, bombing, landslide, destruction of a building, gunfire, contamination of a local area, and similar acts, including technological and nuclear terrorism), but also continuing actions made up of a number of connected attempts against life, health, or property united by a common plan and goal of frightening the population, violating societal security, or putting pressure on organs of power. This element, in our opinion, also differentiates terrorism from other serious crimes.

An example of this would be campaigns of murder and violence carried out among a population on ethnic, religious, or other lines or group armed attacks and mass murders carried out in such forms and using such weapons, means, and methods as are clearly intended to frighten residents and create panic. Such pogroms and attacks can be viewed as single socially dangerous actions aimed at achieving terroristic goals.

It should be emphasized that the goal of affecting decision making by organs of power presupposes a striving to influence both organs of state power (including executive, legislative, and judicial branches, as well as both federal and federation-subject organs) and organs of local self-government, through which the people realize the power pertaining to them in accordance with the Constitution of the Russian Federation. In a criminal-legal assessment of information on facts that might involve the commission of an act of terrorism, it is essential to keep in mind the following circumstances.

In its external aspects and in the socially dangerous consequences it pre-

sents, terrorism resembles certain other crimes against life and health, societal security, and the security of movement and transportation. This concerns such crimes as negligently causing death or harm to health (Articles 109 and 119 of the Criminal Code of the Russian Federation); violating rules of fire safety (Article 219) as well as safety rules at atomic power facilities (Article 215), potentially explosive sites (Article 217), or mining, construction, or other work sites (Article 216); violating rules for the storage and use of explosives (Article 218) or use of transportation (Articles 263 and 268); or handling radioactive materials illegally (Article 220). However, in the cases listed above, the danger to property or human life arises as a result of the negligence of the guilty party. Terrorism here does not represent an intentional crime. An individual committing an act of terrorism recognizes the societal danger of his actions, foresees the unavoidability or possibility that socially dangerous consequences will ensue, and hopes for such consequences in order to achieve his goals.

Terrorism must also be differentiated from certain intentional crimes that are similar from an objective standpoint, such as the intentional destruction or damage of property by universally dangerous means (Part 2, Article 167), the intentional destruction or damage of military property committed by a perpetrator in the course of another military crime (Article 346), or murder committed by universally dangerous means (Article 105, Part 2, Section E). The descriptions of these crimes lack any indication of special terrorist goals. But it is these very goals—the violation of societal security, the frightening of the population, and the influencing of decision making by organs of power—that are pursued by an individual committing an act of terrorism.

The criminal directs his will toward achievement of these goals, and to realize them, he selects the time and appropriate weapons and tools of the crime as well as the situation. As a rule, the terrorist accompanies commission of universally dangerous actions with notification of the authorities and the population that new bombings, arsons, or similar acts are possible. In this way, he is counting on attaining the terrorist goals that have been set. Even mere reports of possible actions that would create the danger of loss of life, significant property damage, or similar consequences are capable of creating panic among the population, producing disorder, disrupting the operations of transportation and other enterprises and institutions, and compelling state agencies to take complex and expensive preventive measures.

It is for this reason that the new Criminal Code classifies as a completed terrorist act even a threat of universally dangerous actions made for terroristic purposes. Furthermore, the making of an intentional false report of an act of terrorism is also deemed to be a crime (Article 207 of the Criminal Code), regardless of the motives and goals of such a report.

A footnote to Article 205 of the Criminal Code concerns the absolution from criminal responsibility of individuals who have participated in preparations for a terrorist act. Its text is practically unchanged from that of a footnote to Article

213/3 of the 1961 Criminal Code of the Russian Soviet Federated Socialist Republic. At the same time, the juridical content of this footnote requires new interpretation. This is due to the appearance in the General Section of the Criminal Code of standards concerning the voluntary refusal of participants in a crime to carry that crime through to completion. In accordance with Part 2 of Article 31 of the Criminal Code, there are no grounds for assigning criminal responsibility to an individual who has voluntarily and finally declined to carry a crime through to completion. Furthermore, an accomplice to a crime bears no responsibility if in addition to voluntarily and finally declining he has also taken all possible measures to prevent the crime. The same would be true for the organizer and instigator of the crime if he in fact managed to prevent the criminal attempt (Part 4, Article 31). It must be emphasized that in this case we are referring not to an absolution of criminal responsibility, but rather to the *complete absence of grounds for such responsibility*.

By comparing Article 31 of the Criminal Code and the footnote to Article 205, one may conclude that the referenced footnote refers only to those cases in which the criminal becomes involved in preventing a terrorist act voluntarily and not through pressure or force (for example, by being discovered and held to account) or because an individual stops a planned terrorist act in order to carry it through later at a more convenient time. In other words, the footnote to Article 205 could be applicable only if there is no evidence of a voluntary and final withdrawal from participation in a terrorist act. If not, then Article 31 would apply, stipulating not an absolution of responsibility, but rather an absence of grounds for responsibility.

In making a criminal-legal assessment of information on planned or completed bombings, arsons, or similar actions, one must make a distinction between a terrorist act and an act of sabotage. Indeed, along with language on responsibility for terrorism, the new Russian Criminal Code also includes a standard on sabotage. Sabotage is defined as a bombing, arson, or other action aimed at destroying or damaging vital service facilities, enterprises, structures, means of communications, or the transportation infrastructure if committed for the purpose of undermining the economic security and defense capability of the Russian Federation (Article 281 of the Criminal Code). Differentiating between the elements involved in these two crimes, terrorism and sabotage, is done by means of objective characteristics (sabotage does not necessarily presuppose the creation of danger of loss of life or serious harm to health, and it does not necessarily require the use of universally dangerous means of harming the above-mentioned facilities) and subjective characteristics (the saboteur pursues certain goals that do not coincide with the goals involved in an act of terrorism).

Sabotage is categorized among crimes against the foundations of the constitutional structure and state security (Chapter 29 of the Criminal Code). According to the law, the fundamental difference between sabotage and a terrorist act lies in the goals of the criminal. A terrorist bombing is directed against societal

security and against the population. It is carried out with the aim of disrupting the foundations for the existence and functioning of civil society, the foundations for the organization and self-organization of the social sphere. If the goal of the criminal is to attack national (state) security and harm its basic values, including first of all its economic security and defense capability, criminal law labels the actions as sabotage. It is no accident that the law does not require the act of sabotage to create the threat of loss of life. Indeed, the saboteur achieves his goals not by frightening the population, but primarily by affecting material objects created and functioning in the interests of protecting the country and defending its economic interests.

The choice of the target that the criminal aims to destroy or damage is the primary evidence indicative of sabotage-related goals. The Criminal Code lists the following possible targets in this category: facilities providing vital services to the population (heating plants, bakeries, medical and pharmacy establishments, water intake sites, etc.); other enterprises and structures; radio, telephone, telegraph, and other communications-related facilities; bridges; roads; means of transportation; and other transport infrastructure-related sites.

Further evidence of sabotage-related goals may be found in the choice of the time, place, and specific circumstances of the crime (for example, the commission of a crime during war or danger of war or during a period of economic crisis, and an attempt to undermine Russian sovereignty using these circumstances). Other evidence may be found in the specific target selected for destruction or damage (for example, a facility that plays a key role in a strategically important economic or vital services sphere). Let us emphasize once more that this sort of case does not require the damage to be caused by universally dangerous means. The means chosen by the criminal are primarily aimed at harming the economy and military power of Russia.

In the course of applying the new Criminal Code of the Russian Federation, a question might arise regarding the possibility of an ideal combination of terrorism and sabotage, that is, a situation in which the perpetrator fulfilled the requirements for committing both crimes in a single action (for example, an action carried out in a zone of internal armed conflict). It seems that the law does not rule out such a possibility. In carrying out his task of weakening Russia's military potential, the criminal takes a defense-related facility out of commission, choosing to use the most terrifying and universally dangerous means and intending to elicit a certain reaction from the authorities.

It should be considered that the law does not rule out the possibility that the criminal may have goals related to both sabotage and terrorism simultaneously. This is possible if, for example, a perpetrator on assignment from a foreign organization and in the aim of undermining the country's economic security takes a strategically important industrial facility out of commission, using means that frighten the population (a powerful explosion) and intending to force the authorities to meet the criminal's individual demands. In such cases, commission

of such a bombing includes characteristics of both sabotage and terrorism, which means that it would be qualified under two different articles of the Criminal Code of the Russian Federation.

When the criminal destroying targets aims to frighten the population so as to diminish Russia's defense capability and its social-moral potential in some manner (for example, in conditions of war or armed conflict), then it is a matter only of sabotage-related goals. No additional qualification of the action as terrorism is required.

Another circumstance also merits attention. In the majority of instances, both acts of sabotage and acts of terrorism are planned and carried out on the basis of a preliminary agreement among a group of individuals or an organized group. It is no coincidence that the Criminal Code includes the appropriate qualifying standards in Parts 2 and 3 of Article 205 and Part 2 of Article 281.

Therefore, it is highly likely that a situation could arise in which the goals of individual participants might not coincide. This is possible, for example, if for the purpose of undermining the economic security and defense capability of Russia, the head of a saboteur group plans a bombing to be carried out by another individual unaware of the group leader's true motives. This individual in fact might be pursuing goals linked with frightening the population or other terrorist purposes. In such situations, the actions of each participant should receive an independent criminal-legal evaluation regarding the orientation of their intentions. The actions of participants in a bombing must be categorized according to the article on terrorism or on sabotage, depending on the goals established and held by each criminal involved.

Examples of terrorism in the political sphere are not found only in universally dangerous actions aimed at influencing the activities of organs of power. Such terrorism can also appear in the form of specific terrorist acts committed for the purpose of halting the political activity of individual persons (Article 277 of the Criminal Code).

Serious changes were made in the 1996 Russian Criminal Code standard on responsibility for terrorist acts. These changes primarily involved characteristics of the objective aspect of the crime. According to the new Criminal Code, a terrorist act is considered to have been committed not only in the event that it causes the death of a state or public figure, but also in the case of attempts on the lives of such individuals. Shifting the moment at which a terrorist act is deemed juridically complete to the assassination attempt stage makes it possible to apply the maximum measure of punishment to the culprit, including the death penalty, even if the intended victim is not killed (although it is true that a death penalty moratorium is currently in effect in Russia).

The list of those potential target individuals who are covered under the crime analyzed above is narrow: the law excludes representatives of organs of power, since responsibility for their murder must fall under Article 295 ("Attempt on the Life of an Individual Involved in Facilitating Justice or Preliminary

Investigations”), Article 317 (“Attempt on the Life of Law Enforcement or Military Service Personnel”), or Part 2 of Article 105 (“Murder in Connection with Employment in an Official Capacity”).

The subjective aspect of the terrorist act has now taken on new characteristics as well. A requisite component of this crime is the motive of revenge for the state or public activity of the victim or the goal of halting the victim’s state or public activity. The above-mentioned motive and goal may be present simultaneously.

The question of types of intent in committing a terrorist act also merits independent evaluation. For Russian criminal law, only direct intent has traditionally been included as a criterion for this crime. This is because the subjective aspect of an act of terrorism for a long time presupposed the mandatory presence of special “counterrevolutionary” or later “anti-Soviet” goals. The presence of this special goal as part of the crime of terrorism understandably narrowed down the possible types of intent, leaving only direct intent. However, the present law also recognizes as an act of terrorism an assassination attempt without any special goal, or only with the motive of revenge for political activity. Thus, “with regard to causing death to the victim, there can be both direct and indirect intent, as the presence of a motive necessarily presupposes direct intent with regard to the action but not necessarily to the result of that action.”

The motive can determine the action itself but can be aimed at another result; in that case, indirect intent is possible with regard to the anticipated result of the terrorist act (death). This occurs specifically if out of revenge for political activity, the criminal wishes to harm the health of a state figure, creating the possibility of his death in the process. In the event that death is actually caused, intent must be considered indirect.

An expansive approach is lacking in recent doctrinal commentaries regarding the concept “state figure.” More accurately, emphasis is placed on the circumstance that the figure is primarily an individual who makes decisions, that is, a leader or member of a collegial governing agency influencing the functioning of the state mechanism or a public association, not merely executing but rather forming their policies.

At the same time, efforts to place only federation-level figures in this category are clearly unfounded. Leaders of cities and districts and similar individuals involved in local self-government must be regarded as public figures, and in this capacity they cannot be excluded from the category of potential victims of terrorist acts.

It should be kept in mind that the new criminal law does not preclude the designation of foreign government officials or figures from international and foreign public organizations as victims under the article on terrorist acts (Article 277), provided that these persons are conducting their activities in our country in accordance with the Constitution of the Russian Federation and Russian legislation.

In conclusion, another new legislative enactment also merits attention. It is commonly known that Part 3, Article 12 of the 1996 Criminal Code of the

Russian Federation sets forth the “real” principle of criminal law activity with regard to actions infringing upon the interests of the Russian Federation.

It signifies that Russian criminal law can be applied to a foreign citizen or stateless person who has committed a crime on Russian soil aimed against the interests of our state. This standard is applied in the event that such an individual is not convicted in a foreign country and is subsequently tried in our country. This means that in accordance with the above-outlined principle in our law, foreigners who have committed the following acts could be held criminally responsible: a terrorist act aimed at influencing the decisions of Russian authorities (Article 205 of the Criminal Code); sabotage of a Russian military or economic target located outside the borders of the Russian Federation (Article 281); a terrorist act against a Russian state or public figure who is temporarily abroad committed in connection with the victim’s official activities but in the interests of our country (Article 277).

From this analysis, it is obvious that the struggle against terrorist activity is effective when it is legal, uncompromising, and correctly qualified, that is, differentiated from other types of crimes that may include elements of terrorization.

Selected Technologies and Procedures Intended to Restrict Unauthorized Access to Explosives

*Bronislav V. Matseevich**

Federal State-Owned Unitary Enterprise
Krasnoarmeisk Scientific Research Institute of Mechanization

I represent the Federal State-Owned Unitary Enterprise Red Army Scientific Research Institute of Mechanization [KNIIM], which works on issues connected with the production and use of civilian explosives, as well as questions pertaining to the dismantling and recycling of munitions.

As noted here earlier in another report, explosions and their sources, explosive substances, are the cheapest and most effective weapons of terrorists. The list of explosive substances now includes more than 2500 items, from the simplest mechanical mixtures of saltpeter with diesel fuel, oil, and so forth, to those for which the manufacturing cycle lasts tens or even hundreds of hours. Explosives today are the bread that feeds industry. Suffice it to say that it takes 500-800 grams of explosives to mine one ton of iron ore, 1000-1200 grams for one ton of coal, and so on. The United States currently produces and consumes more than 3 million tons of civilian explosives annually, more than the amount used during the entire course of World War II by all countries on both sides. In the Soviet Union, the figures reached 2.3 million tons, with the portion lost to theft amounting to less than one-millionth of the total production volume. Today, Russia uses more than 600,000 tons annually. This multimillion-ton genie has been let out of the bottle, and there is no way of putting it back. It would seem that getting hold of 0.01 or 0.001 percent of this amount would not present any difficulty. Nevertheless, even these percentages would amount to tons, and furthermore, terrorists' manuals have long included methods for producing simple explosives themselves.

However, we must keep in mind that on the one hand, the simplest explo-

* Translated from the Russian by Kelly Robbins.

sives are less powerful. On the other hand, using them also requires a detonation intensifier, a so-called intermediate detonator or booster, in the mechanism of the explosive device. Such boosters must be made from powerful explosives such as TNT, hexogen, octogen, and others.

This is necessary because the detonating fuse or blasting cap simply will not detonate the simplest explosives due to their low sensitivity. Therefore, terrorists use powerful explosives such as TNT, hexogen, and plastic explosives in order to achieve a compact and reliably functioning charge.

Thus, the first measures that would help to restrict their uncontrolled spread could be taken right at the factory. I will cite several examples of such possibilities:

1. One such example in Russia is the system for placing serial numbers on cartridges and other products including civilian explosives such as TNT with saltpeter 6ZhV, 79/31, and others.

The mining industry uses about a billion such cartridges annually in 32-, 36-, 45-, 60-, and 90-mm diameters. To limit the uncontrolled spread of these cartridges and related products, each cartridge is assigned an individual number and each blaster must sign for the cartridges he receives, with the numbers being recorded. Thus, if a numbered cartridge is found anywhere, its path can be traced along the entire “producer-consumer” chain, from its manufacture at a plant to a specific mine, warehouse, shift, and individual blaster. All potential sources of losses can therefore be discovered and eliminated.

To put this system into place, 32 special cartridge numbering and packing lines with a capacity of 200 cartridges per minute each were designed, manufactured, and put into operation. All Russian plants producing civilian explosives are equipped with such lines. This is an expensive undertaking, since it entails major costs, detailed accounting, and so forth. But with the introduction of this system in the 1980s, losses and thefts of explosives were reduced to a level of 10^{-6} of total output. Serial numbers are also placed on explosive blocks, boosters, et cetera.

2. A nationwide audit is also conducted regularly regarding the production and consumption of civilian explosives and associated detonating mechanisms. The audit begins with comparing orders from customer firms with inventory logs at the producing plants regarding shipments and utilization of these explosives.

Without a special permit issued on the basis of such an audit, these substances cannot be shipped to customers, stored, or used. The system stipulates strict accountability on the part of producers and consumers. Those providing incorrect information can be held legally responsible, and violations of these rules will lead to loss of licensure by consumers and producers alike.

3. One effective means of limiting the use of powerful explosives in mining is the shift to ammonia nitrate emulsion civilian explosives, which are manufactured at the place of use. This has become a basic method worldwide over the

past decade and should remain so in coming years. Reducing shipment distances by tens of times and shifting to less sensitive explosives significantly limit the base for terrorism. For this purpose, the majority of mining enterprises use domestic- and foreign-designed stationary units for manufacturing explosives.

For this same purpose, Russia also manufactures four types of mixer-loader vehicles, one of which is the so-called factory on wheels, a vehicle in which all basic explosive manufacturing operations are carried out at the blast site during the charge loading process.

4. We attach extraordinary importance to current efforts to add markers or taggants to detect various types of plastic explosives, which are very difficult to detect during shipment inspections.

5. For shipments in dangerous regions, a vehicle has been designed with armored sides to protect against gunfire. The vehicle also has fire-extinguishing features.

6. At present, special attention is being devoted in Russia to matters regarding the circulation of military explosives obtained during the dismantling of decommissioned and obsolete munitions. To this end, a number of efforts have been and continue to be carried out in the Russian Federation based on the fundamental principle that the extraction of high-energy materials from munitions and their reprocessing into civilian explosives must be conducted at special enterprises using special equipment. In this process, powerful military explosives are turned into less sensitive materials by being mixed with additives.

For this purpose, a number of industrial plants and arsenals of the Ministry of Defense have been outfitted with special equipment based on methods developed by Russian specialists. One of these methods is the fundamentally new method of washing TNT-containing explosives with hot organic liquids, for example, paraffin. This causes a significant “phlegmatization” of the resulting recycled explosives, increases the safety of the recycling process, and reduces the sensitivity of the recycled substances. The safety and reliability of the process on the whole has made it possible to create a number of mobile self-powered units mounted in large shipping containers.

An example of such a unit is the modular-container complex for extracting TNT from 76–152-mm artillery shells and recovering TNT fragments at munitions storage facilities. The module consists of three or four 20-foot shipping containers, which can be moved by any means of transport and assembled in the course of 48 working hours. It runs on electricity either by connecting to the local power system or on a 100-kW diesel generator. The TNT output of the complex is 120 kg per hour.

Another example is the modular-container complex for dismantling land mines. It is mounted in three standard 20-foot 1SS or UUK-20 containers. Its TNT output is 240 kg per hour, and from 12 to 20 mines can be processed at once. It can be set up in 40 hours.

The existence of such equipment and its deployment at munitions storage

sites facilitate the additional establishment not only of production controls, but also of controls on the part of the army.

Stationary units have also been developed and put into use for processing munitions with powerful mixed smeltable explosives. One example is a complex for dismantling large munitions, for example, aerial bombs weighing from 250 kg to 9 tons each. The complex has attained product output of up to 500 kg per hour. For this same reason, another complex has been built to dismantle large munitions filled with mixed explosives (for example, torpedo warheads, marine mines, missiles, depth charges, etc.).

The recycling process in all these examples is directly tied to the powerful desensitization of these explosives; that is, it requires 400 grams to 1 kg of powerful boosters to detonate them. Therefore, these substances become ill suited for use in terrorist acts.

To involve specialists and coordinate work in this field, five conferences have been held in the past eight years. Three of the conferences were international, and all of them had representatives from more than 100 organizations.

7. The comprehensive work carried out by KNIIM and a number of Russian organizations has shown the possibility of extracting nonfusible explosives from munitions by the method of hydrocutting and washing with a high-pressure stream of water. Experiments have been done on carrying out this process at pressures ranging from 100 to several thousand atmospheres. On the whole, the setup consists of a pumping unit, the washing unit itself, and a water purification system.

We have drawn some important conclusions regarding the safety of this process. They indicate that there exists a rather broad range of technological parameters for this process, within which hydrocutting and hydrowashing are advantageous for practically all types of powerful high explosives. This also makes possible the radical application of this process in various modified forms for the destruction of explosive packages and various terrorist-produced items in mobile units.

On the whole, we feel that applying various methods and procedures for limiting the uncontrolled spread of powerful explosives by various means—design related, substance compounding related, organizational, technological, and legislative—is an effective though far from comprehensive way of resolving the common problem. Therefore, the domestic policy of high-tech countries must support firms that are working to ensure accountability regarding explosives and related products, organizing product markings that would identify the manufacturer, mothballing explosive capacities in mine blasting zones, and creating less sensitive explosive substances and rapid, lightweight detectors for both explosives and narcotics. Other more reliable methods remain to be created.

Bioterrorism: A View from the Side

*Oleg S. Morenkov**

Russian Academy of Sciences Institute of Cell Biophysics

I work as head of a group at the Russian Academy of Sciences Institute of Cell Biophysics in Pushchino, one of the leading biological research centers of Russia. My work there has been associated with the study of the regulation of monoclonal antibody synthesis by hybridized cells. I have a Ph.D. in molecular biology and a doctor of science degree in virology, and my dissertation focused on the antigen structure of the glycoproteins of the Aujeszky's disease (pseudorabies) virus and the development of serological methods for diagnosing this disease. The Aujeszky's disease virus is a porcine alphaherpesvirus and causes widespread disease in many types of animals, but not in humans. At present, my work is devoted to the study of molecular mechanisms of interaction of the Aujeszky's disease virus with cell plasma membranes.

My research work has never had and does not now have any relation to the development of biological weapons. I have never been involved in the problem of bioterrorism. Furthermore, I have not even taken an interest in this problem.

Recently I was invited to make a presentation at a Russian-American seminar on bioterrorism, to look at the threat of bioterrorism to Russia and the world from the viewpoint of a virologist who has never had any relation to the development of biological weapons, from the standpoint of a scientist living in Russia who is well acquainted with the current status of biology in Russia. I was invited to present my own subjective views on this problem, and I accepted.

Thus, the report that I am presenting is a view of bioterrorism from the side, the view of a nonspecialist in this field who has never been connected with

* Translated from the Russian by Kelly Robbins.

biological weapons, the view of a virologist living in Russia and possessing a certain amount of special knowledge.

Any scientific-technical progress leads to the development of not only positive, but also negative technologies. This leads to improvements not only in the means of supporting life, but also in the means of destroying it. The development of chemistry led to the creation of explosive and poisonous substances, of physics to nuclear weapons, and of biology to biological weapons.

Biological weapons will undoubtedly be very attractive to terrorists of the twenty-first century. In the opinion of specialists, it is already pointless to ask the question, Will terrorist acts be committed using biological weapons? Instead, we face the questions, When will it happen? How can the consequences of such terrorist acts be minimized? How can we reduce the probability that terrorists will use biological weapons?

It seems that bioterrorism is an evil we will have to encounter in the near future, and the entire world community will have to fight it with united efforts.

In my view, the attractiveness of biological weapons for modern terrorists is determined by the following points:

1. We are currently seeing the explosive development of biological science, medical biotechnology, and pharmacology. Increasing numbers of people are working in these fields, and they have the knowledge and qualifications necessary for developing and manufacturing bioweapons. There are also increasing numbers of laboratories and biological and pharmacological production facilities that have the conditions necessary for the production of biological weapons.

2. There is free access to information concerning the manufacture of bioweapons (the culture of viruses and microorganisms, the production of toxins, etc.). Access to this sort of information has become much simpler with the development of the Internet. Even with minimal specialized knowledge, such information is fairly easy to find.

3. The manufacture of biological weapons is relatively easy and cheap. If one has the appropriate strain of a pathogenic virus or microorganism, the pathogen can be cultivated in sufficient quantities without any particular problems in any laboratory possessing facilities for work under sterile conditions. Such conditions are easy enough to create, even at home.

4. The problem of obtaining a pathogenic strain of a microorganism or virus is also solvable, although it might appear to be one of the most difficult problems for bioterrorists. A pathogen might be obtained by bioterrorists by illegal means from laboratories or production facilities where these microorganisms or viruses are being studied or where the corresponding vaccines or test kits are being manufactured. A pathogenic viral or microbial strain could be transferred to bioterrorists by another terrorist group. The important point to remember is that at present, international borders are completely open for the movement of pathogenic strains of microorganisms and viruses. This could happen in the form of an

ordinary letter or sheet of paper containing a dried drop of a pathogenic strain. Viruses can be transported in the form of a dried nucleic acid, which presents absolutely no danger to the person transporting the virus. Once at the destination, cells are transfected with the nucleic acid, and the full-fledged virus multiplies. Thus, a pathogenic strain could be obtained in one place and biomass produced from it in somewhere else, even in another country. If bioterrorists were to develop their own strain using current molecular biological methods, it would require substantial expenditures, and at present I believe this to be unlikely, although possible.

5. Bioweapons are effective in very small doses. The ease of concealing the presence and use of bioweapons, the lack of external evidence at the moment of their use, and the relative ease of their production make it highly unlikely that they could be found and suppressed.

6. Biological weapons make it possible to carry out both individual terrorist acts and mass infections of people, animals, and plants.

7. In my view, the task facing bioterrorists is substantially easier than that faced by the developers of military bioweapons for use under battle conditions. An act of bioterrorism is unexpected. No one is taking countermeasures against it, and it is carried out openly, aimed at unprepared and unprotected people. I believe that the demands made of bioweapons by bioterrorists are significantly lower than the demands made of military bioweapons. Considered ineffective under battle conditions, bioweapons could be very attractive for bioterrorists. Bioterrorists have no need to resolve the problem of stabilizing biological agents or cultivating enormous quantities of them. Even “nonmilitarized” pathogens are sufficient for carrying out an act of bioterrorism.

8. At present, there is practically no technology for protecting against bioweapons that would make it possible to detect and identify a pathogenic microorganism or toxin before it began taking effect. Thus, the fact that an act of bioterrorism had been committed could be discovered only after the victims began to get sick and the illness was identified, which could take a fairly long time, during which a large number of people, animals, or plants could already have become infected.

9. A difficult point in uncovering a case of bioterrorism is the fact that after an outbreak of a certain disease is discovered, it is very hard to say anything about the etiology of the disease. Therefore, if the act of bioterrorism is not of a demonstrative nature and is not announced by the bioterrorists themselves, it is no simple matter to confirm that the premeditated spread of a pathogen has taken place. This is especially true with regard to the spread of diseases affecting animals and plants.

10. Society is neither technically nor psychologically ready for cases of bioterrorism.

Therefore, the relative simplicity of producing biological weapons, the practical invulnerability of the perpetrators, and the possibility of the spread of dis-

ease on a huge scale obviously make biological weapons one of the most attractive tools for terror in the twenty-first century.

All types of bioterrorism are dangerous, whether based on political, criminal, religious, or economic reasons or carried out by mentally ill people. In these various cases, the terrorists are pursuing different goals:

- Criminal bioterrorism will obviously be aimed at specific people or groups of people with the aim of eliminating or blackmailing them; that is, it will be of a localized nature.

- Religious fanatics, separatists, and mentally ill people could probably be attracted by the demonstrative aspect of bioterrorism. Bioterrorism of this type could obviously be of a localized nature or could take the form of a wide-scale terrorist act, which, with good planning on the part of the extremists and the necessary equipment and supplies, could lead to large numbers of victims.

- Bioterrorism could become a means of resolving political problems and destabilizing countries, especially those with already unstable political systems and economies. Terrorist acts involving the widespread release of dangerous human pathogens (smallpox, anthrax) in crowded areas could potentially lead to huge numbers of human casualties and enormous economic costs involved in dealing with the consequences, which could destabilize the situation in a country. This type of bioterrorism is technically the most difficult and requires the dispersion of pathogens in aerosol form. It is necessary to solve numerous technical problems to carry out such an act of terrorism (stabilization of the bioagents, development of a dispersal system, etc.), and it requires a long development period and large investments of money. In the opinion of a number of experts, such a wide-scale act of bioterrorism is unlikely in the near future, if it is not purposefully sponsored by a government that could provide terrorist groups with the finished technology for manufacturing bioweapons.

- Neither can one underestimate economic bioterrorism (the spread of diseases affecting animals and plants). This might serve as a means of waging a competitive economic struggle (including on a scale involving competition between countries). In such a case, certain agricultural sectors could suffer enormous losses, which could lead to destabilization of the countries affected. In the majority of cases, the very fact that such an act of bioterrorism had been carried out could go unnoticed if it is not announced by the terrorists themselves.

In my view, the main factor restraining the spread of bioterrorism is the lack up to now of a sufficiently wide-scale successful act of bioterrorism receiving worldwide attention. Two or three successful acts of bioterrorism, regardless of the country in which they occurred, could change the orientation of terrorists throughout the world and encourage them to actively seek capabilities for using biological weapons for criminal purposes.

What, in my view, are the special characteristics of the situation in Russia with regard to bioterrorism?

- In Russia, there are a large number of institutes and production facilities of a biological, medical, and pharmacological nature. Many of them are in a difficult financial position and sit half empty, rented out to private firms. The laboratory facilities of such institutes and plants could potentially be used by bioterrorist groups to cultivate pathogenic viruses and microorganisms.

- Russia has a large number of specialists—virologists, microbiologists, molecular biologists—with the skills sufficient to be used by bioterrorists for making and developing bioweapons. Some of these specialists are still working in their professional fields and often live on the verge of poverty. Some of them were retrained and now work in other sectors. Here I would like to emphasize that the majority of these specialists were never associated with the development of bioweapons under the old program and are (or were) working on basic or applied science.

Given the poor situation of many scientists working in biology, there is a potential danger that they will be used by criminal elements or terrorist organizations, including those from third countries, in the manufacture of bioweapons. A pathogen can be obtained from any country. There is a potential danger that these pathogens could also be acquired in Russia itself through people with access to pathogenic strains of microorganisms or viruses (for example, people involved in related scientific research or in the production of vaccines or diagnostic tests). For a certain amount of compensation, specialists could cultivate biomass, possibly without even guessing which microorganism or virus they were cultivating.

Russian biologists also could potentially be used by bioterrorists in the development of bioweapons. Despite the difficult situation in Russian science, biological scientists, especially those working in the area of basic science, continue to maintain their high status and to conduct world-class research. Take, for example, a recently published study by Australian researchers that attracted worldwide notice. These researchers cloned the interleukin-4 gene in mouse pox virus and, as a result, unexpectedly obtained a virus substantially more virulent than the initial strain. It is highly probable that cloning such a gene in human smallpox virus could lead to the appearance of a terrible bioweapon. In my view, it would be no particular problem to repeat this work or to insert the interleukin-4 gene in another virus. The work used standard molecular biology methods. Such work could be carried out in many Russian biological institutes, as well as in American universities. Terrorists might plan their work in such a way that one team of specialists clones the virus sequence and another the interleukin gene, a third group makes the recombinant virus, and a fourth tests the virus on animals. None of the researchers could even guess the aim of the work.

- The next important point concerns Russia's lack of modern detection equipment and the associated methodology, thus complicating the possibility of finding pathogenic agents before the moment of their use.
- Russian medical institutions are not prepared to work under conditions that would be produced by bioterrorist actions. Judging from the literature, this problem is also a concern in the United States. There are no specialists trained for such cases, no modern diagnostic methods or equipment for pathogen identification, and no stockpiles of the appropriate vaccines and antibiotics.

In this regard, however, it should be noted that an expert analysis of the current level of preparedness of other countries for acts of bioterrorism shows that, at present, not a single country in the world is fully prepared to take adequate actions in such a situation. A well-planned and successfully conducted wide-scale act of bioterrorism in any country would unavoidably lead to heavy casualties (or enormous damage to agriculture). The scope of the consequences will depend on the preparedness of the government, both technical and economic, for terrorist acts of this nature.

Given Russia's economic weakness and its poor technical preparedness for dealing with the consequences of bioterrorism, a wide-scale bioterrorist attack carried out on Russian soil would in high likelihood produce an unfavorable scenario that might lead to a large number of casualties, social tension, and a destabilization of the situation.

Thus, Russia finds itself in a situation characterized on the one hand by favorable conditions for terrorist groups to make or even develop bioweapons and on the other hand by a lack of preparedness to counter a bioterrorist act if it is committed. In taking all of this into account, it seems to me that Russia could potentially become one of the top places for the manufacture of bioweapons by terrorists (including bioterrorists from other countries). Russia could also become one of the main proving grounds for the testing of bioweapons in terrorist or criminal actions. This cannot be permitted. Having organized the production of bioweapons or having successfully carried out a bioterrorist act in Russia, where it is now easier to do, terrorists will move on to other countries as well.

Russia must become part of the international system for countering bioterrorism. Given Russia's economic problems, it needs help to create an effective system for combating bioterrorism. This is in the interests of the entire world community.

In order to fight bioterrorism, the international community needs to resolve a three-part problem:

1. Society must recognize the seriousness and reality of the problem of bioterrorism. Society has not yet recognized this fact. I fear that society will have to encounter bioterrorism face to face in order to recognize the scale of the danger fully. In this situation, scientists must play the role of experts, who must

convince governments and society as a whole of the need to take appropriate measures.

2. Society must build a system of barriers to block acts of bioterrorism and reduce the likelihood of their being carried out.

3. In case an act of bioterrorism is nevertheless carried out, society must build a system of effective measures that will make it possible to minimize the consequences of these terrorist acts. Since preventing terrorist acts is very difficult, it seems to me that minimizing their consequences should be a top priority.

I will not discuss issues pertaining to the organization of an international system for countering bioterrorism. This is a difficult and complex problem involving a number of fields in which I am not a specialist. I will convey a few more thoughts concerning the potential use by bioterrorists of individual Russian biologists in the manufacture or development of bioweapons on the orders of bioterrorists. It seems to me that the poverty of Russian biological science is the fundamental reason creating the preconditions for the potential use of Russian biologists by bioterrorists for criminal purposes. World-class specialists earn salaries of \$50 to \$100 per month. It is hard to maintain your dignity when you are poverty stricken. In order to earn money, scientists take various side jobs not connected with their basic scientific activities—cloning, sequencing, cultivating biomass, or obtaining recombinant viruses for those who pay them. In doing so, they often have no interest in exactly what they are doing or for what purpose or whom they are doing it. One of the many side jobs being done by Russian scientists could turn out to be an element of work to develop or manufacture a bioweapon. As I have already emphasized, specialists could carry out this work without even having a clue.

In my view, the most effective means of resolving this problem is support for Russian biology on the part of the world community, in particular the United States of America. I would like to stress that serious attention needs to be paid to support not only for military science, but also for peaceful biological science not associated with bioweapons. From the standpoint of potential involvement in the manufacture or development of bioweapons, civilian virologists or molecular biologists are even more attractive to bioterrorists than are military specialists, given the weak control and monitoring research work carried out in civilian biological institutes in comparison with military organizations. I believe that the substantial expansion of the system for grant support of Russian biological science, especially basic biology, and of the system for joint Russian-American projects in biology will be beneficial to both sides and would promote the integration of Russian biology into the world scientific community. In this regard, Russian-U.S. cooperation is possible in the area of basic biological research and in the joint development of means for detecting and diagnosing potential pathogens or toxins that could be used by bioterrorists, as well as means of preventing and treating diseases caused by these pathogens. The more active involvement of

Russian biologists in joint research projects would undoubtedly reduce the probability of their potential use by bioterrorists.

Without a doubt, the development of biological science and biotechnology that we are currently observing will lead in the near future to outstanding fundamental discoveries affecting our understanding of the functioning of certain genes in microorganisms, mechanisms of pathogenesis, and the interaction of viruses with the immune systems of animals. This will make it possible to combat human, animal, and plant diseases more effectively. On the other side of the coin, these discoveries will also lead unavoidably to the appearance of new artificially constructed microorganisms and viruses with greater virulence than the initial strains, pathogens not recognized by the immune system, modified toxins with a high degree of stability, and so forth. At present, bioterrorism based on the use of the latest achievements in molecular biology appears unlikely due to the need for large expenditures and highly skilled specialists associated with terrorist groups. However, within the next few years it could present a colossal problem for the modern world.

In conclusion, I would like to focus attention once again on certain statements included in my report:

1. The relative ease of making biological weapons, the practical invulnerability of the perpetrators, and the possibility of the outbreak of disease on a gigantic scale obviously make biological weapons one of the most attractive tools for terror in the twenty-first century.

2. In connection with the poverty-stricken position of Russian biology, Russia possesses favorable conditions for terrorist groups, including terrorist groups from third countries, to make or even develop biological weapons. In this regard, Russia could potentially become one of the top sites for the manufacture of biological weapons by terrorists. Active targeted support for Russian biological science by the world community, and primarily by the United States of America, would undoubtedly promote the elimination of these negative tendencies.

3. The main factor restraining the spread of bioterrorism is the lack up to now of a sufficiently wide-scale successful act of bioterrorism receiving worldwide attention, regardless of the country in which such an act might occur. An unfavorable situation has developed in Russia, and it might become one of the main proving grounds for the testing of bioweapons in terrorist or criminal actions. This cannot be permitted, because the successful staging of an act of bioterrorism on Russian soil might serve as the starting point for the further spread of bioterrorism. It is essential that an international system for countering bioterrorism be created and that Russia be actively involved in this system.

Electromagnetic Terrorism

*Yury V. Parfyonov**
Institute for High Energy Densities
Institute for High Temperatures

In the first two papers referenced below, specialists of the Russian Academy of Sciences carried out an analysis of the threat of electromagnetic terrorism.¹ It was noted that by using sources of powerful electromagnetic fields and specialized electrotechnical devices, the operations of electro-intensive targets may be disrupted. Distinct from nuclear, chemical, or biological terrorism, these actions leave no tracks; they do not require the terrorists to use means of individual protection. They may be accomplished at a distance from the target or by mobile means.

The problem of the vulnerability of radio-electronic information and control systems to the influence of electromagnetic radiation is an urgent one. Among the most powerful sources of such radiation are nuclear explosions, which, as is commonly known, are accompanied by the generation of an intense electromagnetic pulse. As a result of this pulse, massive failures of radio-electronic and electrotechnical systems occur over a considerable area, as observed in atmospheric nuclear weapons tests in the 1950s and early 1960s. Under current conditions, with microelectronics permeating all spheres of human life and fulfilling important functions, the influence of the electromagnetic pulse of a nuclear explosion would have global and, in a number of cases, catastrophic consequences. An understanding of this danger led to the creation in the late 1980s of Subcommittee SC77C under the auspices of the International Electrotechnical Commission (IEC). This subcommittee was assigned the task of working out a set of standards regulating methods and means for protecting civilian facilities from the electromagnetic pulse of a nuclear explosion. This work is nearing completion. The top-priority area for subsequent activities of the subcommittee will be

* Translated from the Russian by A. Chelsea Sharber.

the development of standards on preventing emergency situations in connection with the threat of unregulated use of nonnuclear sources of powerful electromagnetic radiation.

This decision by IEC is a consequence of the fact that a number of countries now have generators that can produce radiation comparable in intensity with the electromagnetic pulse of a nuclear explosion and would therefore have a more effective impact on radio-electronic systems. The high effectiveness of these generators is explained by the following factors:

1. They emit not a single pulse, as occurs in a nuclear explosion, but a series of pulses repeated with frequencies of up to several thousand hertz.
2. The radiation pulses are more broad-banded than the electromagnetic pulse of a nuclear explosion, and they cover the spectrum of sensitivity of most civilian infrastructure targets.

It should be specifically noted that the construction of super broad-band pulse generators is relatively simple. They may be manufactured in semiprimitive conditions with minimal expense. By this reasoning, analysts predict that these devices will fall into the hands of terrorists, common criminals, and hooligans.² In the opinion of specialists, the consequences of their ill-intentioned or careless use will be extremely serious. Such consequences could include aviation, automobile, and railway accidents; obstruction of radio communications over large areas; disruption of the operations of computer systems in major banks, supermarkets, and control centers; obstruction of technical security systems in major museums, art galleries, vaults containing valuables, and other secured facilities; breakdowns in the operations of the system for controlling electric power facilities; and so forth.

Of course, such predictions require serious examination and, if they are even partially confirmed, the implementation of serious measures to prevent acts of electromagnetic terrorism and to develop methods for eliminating the consequences of emergency situations in the event such acts are perpetrated. A limited study was conducted by specialists from the Institute of Thermophysics of Extreme States of the Russian Academy of Sciences. Two types of experiments were carried out, one investigating the action of super broad-band electromagnetic pulses on computers and the other studying the effect of these pulses on technical security systems. In the course of the experiments, it was established that the computers under investigation failed when exposed to electromagnetic pulses with an amplitude on the order of several hundred volts per meter. This confirmed the prediction about the danger of super broad-band periodic repeating electromagnetic pulses for computer hardware.

The experiments also showed that the following events occurred subject to the amplitude of electromagnetic pulses acting on technical security systems:

1. Failure of the elements of the security equipment;
2. False sensor readings, forcing security personnel to turn off the seemingly defective equipment; and
3. Temporary neutralization of security systems.

The last possibility calls for special concern, since it involves the likelihood that a criminal could get past the security system without sensors' making the appropriate signal to the central control station.

Apart from experiments utilizing the super broad-band electromagnetic pulse generator, the possibility of perpetrating terrorist acts using simpler and cheaper means was also investigated. One such means would be a high-voltage pulse generator. A set of theoretical and experimental investigations was carried out regarding the way in which this voltage permeates computer systems. The five-story building in which the institute is situated was chosen as the site of the investigation.

The goal of the work was to demonstrate the possibility of causing a considerable number of computers to fail by hitting them with pulses of current through the power supply and grounding circuits. Moreover, the points of entry for the pulses were located outside the building. According to the results of this work, it is possible to confirm that the electric power supply and grounding circuits represent an effective channel for the permeation of electrical pulses into the building, despite the presence of voltage limiters and filters. The test signals reached computers in the building practically without weakening, and in a number of cases the signals were even strengthened as a result of resonance phenomena. Estimations indicate that the failure of practically all the computers in the building could be caused by using a 10-100-kV pulse generator linked to the power supply and grounding circuits of the institute building.

In addition to the aforementioned experiments, the parameters of the grounding system in a major telecommunications center were also measured. A considerable imbalance was discovered in the parameters of the grounding devices of different receiving and transmitting stations. As a result, even at minimal (measured) levels of probing signals, failures were observed in the operations of the digital telecommunications system. There is no doubt that with a feed of pulses from 10-100 kV, these systems will fail.

Thus, it is possible to state that effective technical means of protection against electromagnetic terrorism must be developed. It may be necessary to review and enhance rules regarding grounding devices and the laying of power cable. In any case, research should continue, and immediate measures should be developed and implemented. Such efforts will be even more useful, given that they will increase the stability of electronic systems against any electromagnetic obstacles, including lightning discharges, discharges of static electricity, et cetera. Inasmuch as terrorism has taken on an international character in recent years,

causing serious anxiety in all industrially developed countries, it would be expedient to take measures to facilitate international collaboration in this area. Among other possible efforts, it is necessary to organize a joint experiment on assessing the real danger of electromagnetic terrorism and developing means of protection.

NOTES

1. Fortov, V.E. 2000. About the potential possibility of commitment of large-scale terrorist acts by using electrotechnical devices. EUROEM 2000, Edinburgh, May 30-June 2, 2000.

Fortov, V.E. 2001. A computer code for estimating pulsed electromagnetic disturbances penetrating into building power and grounding circuits. 14th International Zurich Symposium on Electromagnetic Compatibility.

2. Schriener, D. 1998. The design and fabrication of a damage inflicting RF weapon by "back yard" methods. Statement before the United States Congress Joint Economic Committee, Wednesday, February 25, 1998.

Russian Legislation and the Fight Against Terrorism

*Viktor E. Petrishchev**
Russian State Duma

In the early 1990s, terrorism in the Russian Federation underwent a transformation from a number of unrelated, rare, and somewhat unique manifestations of violent crime to a systemic and large-scale threat to the state and society in general. Prior to that period, the Soviet Union had legislation in place that provided for rather harsh repression of socially and politically motivated criminal acts. Therefore, potential perpetrators of terrorist acts (such as ultranationalists, religious fanatics, and extremists) who were plotting violent changes of the existing sociopolitical order, and so forth, were usually identified by law enforcement agencies in the early planning stages. Potential perpetrators were subjected to open and clandestine operations aimed at correcting their behavior and redirecting their activities into legitimate channels. In addition, the nationwide system for preventing extremist and terrorist acts seemed to be quite effective. For instance, the distribution of anticonstitutional propaganda and the creation of organizations for this purpose were punishable under the Criminal Code. State censorship eliminated possibilities of mass production and legitimate dissemination of materials proclaiming ideas of national, religious, or racial superiority; licensing and permit requirements created serious obstacles to procuring firearms and explosives.

Given all of the above circumstances, the few isolated terrorist acts that occurred, such as the bombing of the Moscow Metro perpetrated in 1977 by a group of Armenian nationalists and the hijacking attempt by a group of youths in Tbilisi Airport in 1984, were justifiably considered to be unique occurrences, atypical for our country. As a result, only two types of crimes were classified as terrorism under the Soviet legislation of that period: a terrorist act and a terrorist

* Translated from the Russian by Rita Kit.

act against a representative of a foreign state (Articles 66 and 67, respectively, of the Criminal Code of the Russian Soviet Federated Socialist Republic [RSFSR]).

However, by the early 1990s the situation had changed considerably. Riding on the wave of the so-called democratic reforms, the country experienced an outbreak of destructive processes creating a favorable environment for increased crime, extremism, and terrorism. Among these factors were economic decline, deterioration of interethnic relations, growth of separatism, and loss of the values that formerly bound the society together, such as civic duty, patriotism, and internationalism. While the head of state, Mikhail Gorbachev, traveled overseas promoting his new policies and universal human values, his very own state was collapsing. Overall, the self-centeredness and nearsightedness of those at the highest levels of political office, the lack of executive control over developments in the outer regions of the USSR, and the political manipulation of various nationalists and extremists by a new breed of ambitious politicians seeking to seize political control resulted in the breakdown of law enforcement. Unauthorized meetings, demonstrations, and marches became more prevalent. They increasingly took on an antisocial nature and more frequently turned into riots and civil unrest. The Kremlin failed to respond swiftly and decisively, and as a result, law enforcement and the military were held hostage by an indecisive head of state. Eventually, these processes resulted in the *de facto* collapse of the state.

However, a new political “elite,” actively employing nationalistic and separatist ideas as well as political and religious extremism in their political fight with the central authorities, failed to recognize the fact that the destructive processes they had supported so actively were gaining a substantial momentum of their own. Having achieved widespread support among various groups of the population, extremism turned into a considerable threat to the newly emerging post-Soviet administrative and political entities. Underestimation of this threat by the leaders of the newly created states, illustrated by Boris Yeltsin’s appeal to the subjects of the Russian Federation “to take as much sovereignty as they can possibly swallow,” resulted in a number of large-scale conflicts, some of them armed.

Widespread legal and moral nihilism and the loss of general social values and spirituality greatly contributed to increased incidents of terrorism in Russia and other members of the Commonwealth of Independent States. In addition, on numerous occasions, the highest authorities themselves demonstrated a total disregard for the rule of law and the national constitution. Illegal violence was regularly employed by those in power to protect some unclear “vital interests” (as defined by the head of state and his closest staff). In the Russian Federation, this trend reached its peak in October 1993, when the Russian “White House” was assaulted in Moscow.

One can argue that the above comments go far beyond the scope of discussing Russian antiterrorism legislation and venture into the field of political science, but I felt obligated to bring them up here, given the truly decisive role these negative developments played in the late 1980s and early 1990s.

Other factors contributing to the spread of terrorism in the Russian Federation in the early 1990s include the following:

- Overall decline in economic activity;
- Increased tensions in interethnic relations, frequently resulting in armed conflicts of varying intensity;
 - Increasing numbers of social problems—unemployment, declining material well-being of the active work force, lack of a targeted youth policy, loss of ideological and moral values;
 - Weakening of the licensing and registration system for weapons and an increase in illegal trafficking in firearms and other aids to violent crime;
 - High level of corruption among government bureaucrats, resulting in a rise in both organized crime and street crime; and
 - The relationship between religious and political extremism on the one hand and increased overall levels of criminal activity in society on the other.

In this context, starting in the early 1990s, statistics in the Russian Federation showed a steady increase in crime. For example, during 1994-1995, only 64 bombings were reported, but during 1996-2000, the annual number of such explosions was 600-700 (155 such cases were reported in the first quarter of 2001). Special attention should be paid to changes noted in the nature of crimes committed using explosive devices. Most frequently, these crimes do not fall into the trivial “gang warfare” category, but rather seem to meet all of the criteria of terrorist acts. According to the Federal Security Service of the Russian Federation (FSB), only 16 out of the total number of 600 reported bombings in 1997 could be treated as terrorist acts, while out of approximately the same number in 2000, 150 could be considered terrorist acts. Using the same criteria, 61 of the 155 bombings in the first quarter of 2001 were deemed to be terrorist acts.

In addition, one needs to emphasize a trend toward increasing human and social impacts of the bombings committed in the Russian Federation in recent years. For instance, in 1997, 153 lives were lost as a result of bombings; in 1998, 163; in 1999, 506; and in 2000, 207, with hundreds more wounded. So far this year, dozens have been killed or injured.

In the mid-1990s legislators had to respond to the growing threat of terrorism and to broaden the definition of criminal acts classified as terrorism. Adopted on January 7, 1994, Federal Law 10-FZ introduced into the RSFSR Criminal Code Article 213(3), entitled “Terrorism.” This marked the first legal definition of the term terrorism in our country. The article defines terrorism as “bombings, arson, and other acts causing a threat to human life, major property loss, and other negative consequences committed against public safety or with the aim of influencing decision-making of the government authorities.”

The new Criminal Code of the Russian Federation, which came into force on January 1, 1997, defines terrorism in Section IX, Chapter 24 (crimes against

public safety and public order), Article 205. In my opinion, the primary aim of terrorist attacks is much broader than public safety—terrorists commit their acts against the constitutional foundations of society and its governing structure. Therefore, it would have been more appropriate to include the article on terrorism in Section X of the Criminal Code, which deals with crimes against government authority. Indeed, are the consequences of a terrorist act less significant to the state and society than an attempt on the life of a law enforcement officer? The law punishes an attempt on the life of a law enforcement officer with the death penalty, while committing a terrorist act (without aggravating factors) carries a sentence of only five to ten years of imprisonment.

The definition of terrorism in Article 205 seems to be incorrect as well. In this article, terrorism is defined as “bombings, arson, and other acts representing threats of loss of life, major property loss, and other negative consequences, provided that these acts were committed against public safety, with the aim of spreading fear among the population or influencing decision-making of government authorities, and/or a threat of committing these acts with the same purpose.”

An analysis of this definition shows that it fails to adequately describe the nature and substance of terrorism. In fact, terrorists may pursue goals that go beyond influencing the decision making of government authorities. According to M.P. Odessky and D.M. Feldman, terrorism, in its broadest possible definition, is “a way of governing society through fear.”¹ Therefore, terrorists may also target people outside the government. The targets can be based on nationality, race, politics, economics, religion, or some other criteria; in some cases an entire population can be targeted.

I would also like to question defining “spreading fear among the population” as the primary objective of terrorism. Indeed, spreading fear among the population is a very important component of terrorism. (The authors of the Article 205 of the Criminal Code of the Russian Federation should be credited with mentioning this component—it was not included in the body of Article 213[3] of the RSFSR Criminal Code.) However, this component serves merely as a tool for achieving terrorist objectives and is not an ultimate goal by itself.

Finally, the text of Article 205 of the Criminal Code fails to adequately reflect the substance of terrorism, even when taken not as a sociopolitical phenomenon, but as purely a criminal one. One can easily see that in this article, the legislators provided a list of various manifestations of terrorism—arson, bombings, and other acts. Therefore, the title “Terrorist Acts” would have been more appropriate for this article, rather than the present title, “Terrorism.” This substitution of definitions resulted in a number of difficulties in drafting the Federal Law “On Combating Terrorism,” which is described below.

The institution of criminal penalties for terrorist acts nevertheless failed to address the problem of terrorism as an extremely dangerous sociopolitical phenomenon. (In addition to Article 205, “Terrorism,” the Criminal Code of the Russian Federation contains Article 206, “Hostage Taking”; Article 207, “Mak-

ing Knowingly False Statements About Terrorist Acts”; Article 277, “Attempt on the Life of a Government or Public Figure”; and Article 360, “Attack on Persons and/or Entities Enjoying International Protection.”) The need for a comprehensive nationwide system of counterterrorist measures was first realized in the early 1990s by the agencies most familiar with terrorist acts, namely, the security services and law enforcement. In late 1996, a working group charged with drafting the Federal Law “On Combating Terrorism” was created under the auspices of the Committee of the State Duma. The Chairman of the Duma, Mr. V.I. Ilyukhin, headed the working group. Although the working group was rather small in number, dozens of scientists, experts, and practitioners from various ministries and agencies contributed to the final draft. In addition to several documents already prepared by the Federal Security Service, Ministry of Interior, and Office of the General Prosecutor of the Russian Federation, the working group studied materials from a number of conferences held on this topic and the legislation of some foreign countries, including Great Britain, Israel, Spain, Italy, Peru, the United States, Turkey, and Germany. I would like to emphasize that the vast majority of Duma deputies, regardless of their party or political affiliation, supported the activities of the working group. I believe that this overwhelming support can be explained by the fact that terrorism is an “equal opportunity” threat—it makes no exceptions for race, class, nationality, or ethnicity. As recent history has shown, victims of terrorist attacks can be found among heads of state, public figures, entrepreneurs, and innocent passersby.

By the time of the first reading of the draft on September 10, 1997, terrorism was defined by the authors as a sociopolitical phenomenon manifested through “illegitimate violence (or threat thereof) against persons and entities or destruction/damage (or threat thereof) of property committed with the aim of undermining public safety, international entities, and the established system of national government through forcing government bodies to make decisions desired by the terrorists.” In this wording, the authors clearly stepped aside from the narrow legal definition of the term—and they were perfectly right to do so, since this is not a criminal law, but a federal one, designed to establish a nationwide approach to combating terrorism as a dangerous sociopolitical phenomenon. This is the wording that was adopted almost unanimously by the deputies of the State Duma during the first reading of the draft law.

However, during the comment stage, the authors received substantial number of similar comments² urging them to bring the definition into accordance with the wording of Article 205 of the Criminal Code of the Russian Federation. Among others, the President and the Government of the Russian Federation submitted similar requests. Unfortunately, the influence and authority of those commenting prevailed, and the definition was subsequently narrowed down to a mere list of terrorist acts as described in Articles 205, 207, 277, and 360 of the Criminal Code. This change inevitably resulted in the narrowing of the statewide prevention role. On the one hand, changes in the definitions shifted the emphasis

toward combating terrorist crimes, which fall under the jurisdiction of the security services and law enforcement agencies. On the other hand, the narrower definition removed a number of factors from their focus, which played an important role in defining terrorism itself. However, these factors have to be addressed not only from the legal standpoint, but also through a nationwide system of economic, social, ideological, and other measures.

I must bring to your attention yet another shortcoming of the draft, which appeared after it was adopted at the first reading on September 10, 1997. This issue relates to the status of the Federal Interagency Anti-terrorist Commission, which was created by the Russian Federation Government Decree 45, dated January 16, 1997. The director of the Federal Security Service of the Russian Federation was appointed to head the commission, whereas in most other countries antiterrorist activities are conducted under the auspices of the highest executive office in the nation. This status would have been very beneficial in present-day Russia. That is why the authors of the Federal Law in the article titled "Interagency Antiterrorist Commission of the Russian Federation" provided that the Government of the Russian Federation would create the commission and the deputy chairman of the government would head it. The same article provided a relatively detailed outline of the mission statement, authority, and responsibility of this federal coordinating body. In addition, the law provided for establishing similar bodies at the federation subject level (or regional level, including several federation subjects). All of these measures were reflecting the proposed nationwide vertically integrated system of antiterrorism measures. Unfortunately, given persistent requests from the Office of the President, this provision was changed as follows: "To provide for proper coordination of anti-terrorist activities, the President and the Government of the Russian Federation may set up regional and federal antiterrorist commissions."³ Only later was this corrected (Russian Federation Government Decree 1302, dated November 6, 1998). The decree also appointed the chairman of the Government of the Russian Federation to head the commission.

In the final analysis, the Federal Law "On Combating Terrorism" that went into effect on August 4, 1998, remained an imperfect document. However, it contributed to solving a number of earlier problems. It provides for certain legal and social guarantees for individuals directly involved in counterterrorist operations. This provision was especially important for law enforcement officers. The law also establishes clear definitions and introduces major terms, which is helpful not only for the theoretical analysis of the situation, but also for the practical work of several executive agencies, the security apparatus, and the general public.

The law provides a clear list of entities directly responsible for counterterrorist operations. Article 6 establishes that there are six such agencies in the Russian Federation: the Federal Security Service, the Ministry of Internal Affairs, the Foreign Intelligence Service, the Federal Protective Service, the Ministry of Defense, and the Federal Border Service. Unfortunately, their respective

jurisdictions were not clearly defined. For example, Subarticles 2 and 3 of Article 7 provide that prevention, identification, and investigation of politically motivated terrorist crimes fall under the jurisdiction of the Federal Security Service, while prevention, identification, and investigation of financially motivated terrorist crimes fall under the jurisdiction of the Ministry of Internal Affairs of the Russian Federation. However, the law fails to provide clear definitions and a distinction between political and financial motivations.

The law also stipulates that in addition to the above-listed agencies, the Government of the Russian Federation provides a list of other federal executive agencies that may be called upon to contribute to counterterrorist activities within their respective competencies.

Establishing the list of specific ministries and agencies directly responsible for counterterrorist activities is important, and it is far from being a mere formal declaration. One should take into account the fact that at the earlier stages of drafting this law, heads of some of these bodies attempted to rid themselves and their agencies of this responsibility, arguing that this function was not delegated to them under earlier legislation. Had this position prevailed, the legislators would have been forced to delegate this responsibility to two agencies only—the Federal Security Service and the Ministry of Internal Affairs of the Russian Federation. Indeed, prior to drafting the Federal Law “On Combating Terrorism,” these two agencies were the only ones responsible for such activities (see Federal Law 40-FZ “On the Federal Security Service of the Russian Federation,” dated April 3, 1995; Federal Law 27-FZ “On the Internal Troops of the Ministry of Internal Affairs of the Russian Federation,” dated February 6, 1997; and Decree 1039 of the President of the Russian Federation “On Approving of the Regulations Regarding the Ministry of Internal Affairs of the Russian Federation”). The authors of the Federal Law “On Combating Terrorism” based their work on the assumption that the new law can modify agencies’ responsibility in accordance with the earlier enacted legislation.

Chapter III (“Management of Counterterrorist Operations”) of the Federal Law “On Combating Terrorism” deserves positive mention as well. This chapter provides a general outline for establishing and managing task forces for conducting counterterrorist operations, which brings much needed clarity into mounting and running such operations. The commander of the task force is given broad authority—he decides on the scale and scope of the operation, determines the timeframe of the operation, determines what forces and assets will be utilized, determines what kind of information is given to the media, et cetera. The article “Management of Counterterrorist Operations” specifically provides that “interference by any person regardless of his/her position in the day-to-day management of the counter-terrorist operation is strictly prohibited.” The provisions of Chapter 3 passed real-life tests during the special counterterrorist operations in Chechnya, when the Federal Law “On Combating Terrorism” de facto replaced the failed Federal Law “On Emergency Situations.”

The Federal Law “On Combating Terrorism” also imposed severe restrictions on deals that can be offered to terrorists in order to save human lives. Should negotiating with terrorists be deemed necessary, negotiators must be specifically authorized by the task force commander. No individuals can be turned over to terrorists, no weapons or hazardous materials can be given to them, and no political demands could be considered in exchange for calling off the terrorist act.

Finally, the law attempts to break away from the recent trend of narrowing the definition of counterterrorism to a mere response to terrorist acts. (Once again, deficiencies must be pointed out in the definition of terrorism used in the language of Article 3 of the Federal Law.) Nevertheless, immediately after declaring the principle of the rule of law, Article 2 (“Fundamental Principles of Combating Terrorism”) of the Federal Law states that “priority shall be given to terrorism prevention.” The goal of terrorism prevention is emphasized numerous times in other provisions of the law, along with the need for obtaining timely information about the planning and preparation of such attacks.

There is no need to argue that when facing terrorist acts, law enforcement officers are facing the consequences of chronic processes that lead to crime, processes that are outside their direct control. These include social, political, and economic developments, interethnic relationships, relationships between the federal government and federation subjects, and so forth. Therefore, the law makes an attempt to shift the emphasis to terrorism prevention, including holding government officials liable for poor administrative and political decisions.

Let me elaborate on the previous statement. The primary causes of terrorism in modern Russia lie in the current economic and social crisis, worsening interethnic relationships, and increased political tensions. Therefore, any terrorist act is a result of the dynamic interaction of adverse societal conditions and personality disorders, usually attributed to the perpetrators of terrorist acts. I dare say that there is a trend perfectly illustrated by both international and Russian experience. When the national economy is stable, the government’s social policies are well balanced and supported by the majority of the population and people’s incomes are far above the poverty line. When an individual can freely and fully satisfy his or her spiritual and material needs and exercise his or her rights and freedoms, there are no adverse societal conditions feeding terrorist acts, and personality disorders become the primary motivation. On the contrary, when the national economy, social policy, and spiritual well-being are suffering from a major crisis, terrorist acts are driven primarily by these adverse conditions.

Psychologically motivated terrorist acts could be best illustrated by the actions of Theodore Kaczynski (labeled by the Federal Bureau of Investigation [FBI] as the Unabomber), who terrorized the entire United States from 1978 until 1985, or Charles Whitman, whose 1966 shooting spree in Texas left 12 dead and 30 wounded.

On the other hand, the increase in terrorist activity in Russia over the past

decade can be explained primarily by adverse societal conditions. Their combined effect is largely responsible for the outburst of terrorism in Chechnya as well.

Given the fact that terrorism is becoming an increasing threat to countries all over the world, many nations are actively seeking ways to enhance their national antiterrorist legislation. Obviously, in spite of the increasing trend toward globalization, each country is searching for its own unique ways of protecting itself against terrorism. In light of this, studying international experience in the area of counterterrorism policies, approaches, and regulatory framework is becoming increasingly important. Such studies provide researchers with a set of tools and techniques, enabling them to better analyze the threats facing their own countries and to devise the most effective nationwide systems for preventing and eliminating terrorism.

In fact, despite the diversity of national legal systems and approaches to terrorism prevention, most were developed in response to the same fundamental set of internal and external factors. These include the nature of the external threat, the domestic political situation, crime levels in the country, the nature of long-term domestic conflicts, the history of various ethnic groups and their cultural and religious traditions and norms, the level of cultural and legal awareness of the population, the development of the societal institutional framework, and so forth. Analysis of the impact of the above-mentioned factors on the development of antiterrorist legislation in various countries and application of this international experience to the specific circumstances in your country may result in development of the most effective model for a national approach to combating terrorism. Implementation of this approach while fully utilizing international experience may save time on empirical testing of various models and may raise the level of academic research and practical work in your own country to a higher level.

Comparative studies of antiterrorist legislation and law enforcement practices throughout the world enrich all specialists, enabling them to view the problem in its entirety, thus putting them in a position to propose promising approaches for enhancing national legislation in this area.

Let me briefly touch upon Russian and American approaches to combating terrorism, which I hope will be interesting given the topic of our seminar. To save time, I will not go into a detailed analysis of the causes of terrorism in our two countries, because this issue could become a subject for a separate discussion.

Mr. David Tucker, who has specialized in research on special operations and low-intensity conflicts over the past 25 years for the U.S. Department of Defense, has outlined the following principles of antiterrorist operations:

- Following a policy prohibiting deal-making with terrorists;
- Expanding the jurisdiction of national legislation to allow for the pursuit of terrorists outside of the United States;
- Actively promoting international antiterrorism conventions and treaties;

- Designing and implementing various defensive antiterrorism measures;
- Attacking the causes of terrorism and preventing it from spreading;
- Implementing forward-looking measures designed to prevent terrorist acts; and
- Carrying out special operations to destroy terrorist organizations from within.⁴

There are similarities in the antiterrorism policy of both Russia and the United States, including restrictions on mass media coverage of terrorism-related events; possible deployment of military assets to respond to large-scale terrorist acts; utilization of undercover methods to penetrate terrorist organizations; social guarantees and protection of personnel involved in antiterrorist operations; et cetera. Analysis of the principles of antiterrorism policy outlined in Article 2 of the above-mentioned Russian Federal Law reveals the following similarities:

- Rule of law;
- Higher priority for terrorism prevention;
- Inevitability of punishment for terrorist acts;
- Combination of transparent and undercover methods;
- A comprehensive approach, including preventive measures, political, legal, socioeconomic, and public relations actions;
- Priority protection of the right of victims of terrorism;
- Minimal yielding to terrorist demands;
- Single line of command for counter-terrorist operations; and
- Minimal reporting of tactics and methods of counterterrorist operations, as well as minimal disclosure of information about the personnel involved.

A comparative analysis of the Russian Federal Law “On Combating Terrorism” and the U.S. Antiterrorism and Effective Death Penalty Act of 1996 shows some common features, despite major differences in the two documents. For example, U.S. and Russian legislators give different definitions of terrorism; they differ in their identification of the primary causes of terrorism; and they give the government different authority to deal with external threats. In addition, the legal framework is different in the two countries. Besides, the Antiterrorism and Effective Death Penalty Act is a very detailed document, while the Russian law is relatively short (containing only 29 articles) and provides only general regulation of counterterrorism activities.

Obviously, the financial resources of these two nations are vastly different. In fact, the adoption of the U.S. Antiterrorism and Effective Death Penalty Act resulted in additional multimillion-dollar appropriations to the agencies involved in counterterrorism work, including the FBI, U.S. Customs Service, Immigration and Naturalization Service, Drug Enforcement Administration, Departments of Justice and Treasury, U.S. Secret Service, and others. To illustrate the Russian

situation in this area, let me provide the following examples. In the beginning of 1999, the Security Council of the Russian Federation acting in accordance with the decree of the President, drafted the Federal Program on Strengthening Counter-Terrorism Activities. Having “cleared” all stakeholders (i.e., agencies directly involved in this work), the draft was then “killed” by the Ministry of Economy and the Ministry of Finance because there were no funds to pay for the proposed measures. It should be noted that preventive measures were prevalent in that program, with special emphasis on active countermeasures against the dissemination of extremist and terrorist ideologies. I believe that the absence of these measures contributed to the failure of attempts to combat the Wahhabi and Chechen separatist agendas, which drew Russia into a long-term armed conflict in the North Caucasus region.

To continue discussing the importance of preventive measures, one cannot help but appreciate the strong preventive components built into the U.S. Antiterrorism and Effective Death Penalty Act. For example, in this act, American legislators demonstrated their deep understanding of and concern over newly emerging terrorist threats involving modern technologies. Building upon detailed models of potential terrorist threats involving weapons of mass destruction, the act provides for a number of measures aimed at preventing such terrorist acts, which could possibly lead to massive loss of human life.

Potential terrorist acts involving the use of explosives and modern weaponry and technology may be prevented by imposing strict regulations requiring the proper safeguarding and storage of materials that could be used to carry out terrorist acts. In addition, the law imposes criminal charges for activities conducted in preparation for committing a terrorist act or creating a favorable environment for it. For example, Article 503 obligates the Attorney General and the Secretary of Defense to exercise personal oversight over thefts of firearms, explosives, and other hazardous materials and to report their findings to Congress.

Article 511 imposes harsher punishments for illicit trafficking in weapons-grade biological materials and imposes stricter regulations on their storage and use for scientific research. In particular, the Secretary of Health and Human Services is required to compile, approve, and update as necessary a list of potentially dangerous biological preparations. The Secretary is also responsible for designing and enforcing safety rules for dangerous biological materials, for ensuring that personnel working with these materials have the proper training and retraining, for providing adequate equipment and establishing proper procedures for secure storage, and for designing countermeasures to neutralize potential threats in the event of theft.

Section VI of the act regulates enforcement of the Convention on Plastic Explosives. This is very important, since these explosives are extremely powerful and difficult to detect with scanning equipment. Several measures were built into the law in order to prevent the commission of crimes with this type of explosive. Article 603 (mandatory identifier) imposes criminal penalties for man-

ufacturing plastic explosives without special identifying ingredients. Criminal penalties are also imposed on the export, import, possession, transportation, and receipt of unidentifiable explosives. Violators can be punished with up to 10 years in prison.

There are several other examples of preventive measures built into the act, which should be of great interest to Russian legislators.

At the same time, strengthening preventive measures is by no means the only method of enhancing Russian antiterrorist legislation. There are several other problems that have to be addressed. For example, there is a great need to extend the period that individuals reasonably suspected of belonging to terrorist organizations can be detained by the authorities. There are several provisions of the criminal law effectively nullifying the principles of inevitability of just punishment that are no longer acceptable in the present situation. In general, the Russian public fails to understand why a terrorist whose atrocities were documented, witnessed, and proven in a court of law should remain reasonably certain that the maximum penalty is life in prison. Members of the public wonder why the government is sending the message that it is safe to commit even more murders. They ask what happened to the principle of adequate punishment. Why spend taxpayers' money to feed "scumbags" covered in the blood of countless victims? Is it not time to suspend the moratorium on capital punishment for individuals who were found guilty of intentionally killing large numbers of people? I believe that in this regard we have a lot to learn from our American colleagues. Let me remind you of the name of the corresponding American law—the Antiterrorism and Effective Death Penalty Act! The Russian law has serious loopholes in the area of preventing and responding to high-tech terrorism as well.

I believe that the American side can also benefit from an analysis of the appropriate Russian legislation and its application to operations in Chechnya, especially taking into account the fact that the United States has had a long and difficult history of dealing with Islamic extremists of the type currently operating in Chechnya.

In conclusion, I would say that enhancing national antiterrorist legislation, bringing it into compliance with the norms of international law, and harmonizing national approaches toward combating terrorism and reducing terrorist threats appear to be the most promising methods available to the international community to fight terrorism.

NOTES

1. Odessky M.P., D.M. Feldman. 1997. *The Poetry of Terror and the New Administrative Mentality*. Moscow: Russian State Humanitarian University, p.19.
2. More than 300 comments and amendments were offered after the first reading of the draft.
3. President's Comments on the Draft Federal Law "On Combating Terrorism" (No. Pr-1705, October 18, 1997).
4. *The Washington Quarterly*. 1998, No. 1.

Could Terrorists Produce Low-Yield Nuclear Weapons?

*Stanislav Rodionov**

Russian Academy of Sciences Space Research Institute

Quite recently, most specialists have implied that terrorists would try to produce nuclear weapons using existing scientific knowledge and technical potential. For example, the Committee on International Security and Arms Control (CISAC) of the U.S. National Academy of Sciences came to the following conclusions concerning the unauthorized use of plutonium:¹

- Possible proliferators could produce nuclear explosive devices even from reactor-grade plutonium; a simple design (i.e., implosive systems) would provide a yield from one to a few kilotons, while a more modern design could provide a higher yield.
- In assessing security threats, it is necessary to understand who is trying to acquire and misuse plutonium. Terrorists might care little about the differences between reactor-grade and weapons-grade plutonium. Small nations would be likely to care more, in the sense of preferring to make weapons from weapons-grade plutonium, if everything else were equal.

I would like to focus on the fact that the situation might be much simpler. Indeed, although terrorism in general is an unpredictable and uncontrolled phenomenon, nuclear terrorism itself may have some specific features.

First, it might be dangerous and risky to keep stolen nuclear explosives for a long time. In this case, one could not spend the extra time needed to develop (not to mention, test) a reliable nuclear bomb. It is highly probable that terrorists

* Translated from the Russian by Kelly Robbins.

would need just an explosive device—and a very simple device at that—to carry out a single action.

Second, the explosion itself might be the most effective factor in achieving the terrorists' objectives, rather than the nuclear blast yield. Moreover, an enormous number of victims could have a negative effect on that part of the international community that adopts a positive or neutral attitude toward terrorists.

Therefore, low-yield nuclear explosive devices might be rather attractive for terrorists, barring any serious technical barriers to their construction. We shall see later that under some conditions this problem may have a solution.

Let us consider two approaches to lowering the yield of a nuclear explosion. The first is based on extremely high compression of a fissile material. It is well known that its critical mass is inversely proportional to the square of its density. For example, plutonium density in modern weapons designs is three to four times higher as a result of implosion.² At higher compressions, there is no limit on the minimum amount of fissile material required to construct a nuclear explosive. One can imagine micronuclear explosives with yields in the ton range, requiring fissile materials on the order of hundreds or even tens of grams. But what can actually be achieved along this line of development is limited only by available implosion technologies. Thus, it does not seem that this straightforward approach could be used by terrorists, because it requires a very high degree of technical expertise.

The other approach is connected to the so-called fizzle effect, which really is a preinitiation of a nuclear chain reaction in a fissile material in a supercritical state (due to the occurrence of "accidental" neutrons). As a result, the yield of the explosion is reduced in comparison with its nominal value. It should be noted that all types of nuclear weapons have a nonzero fizzle probability. One can categorize all types of nuclear weapons as either fast (implosive systems) or slow (gun-type assemblies) depending on the "waiting time" between the start of criticality and the moment of optimal condition. The fizzle effect is more probable in slow systems and for fissile materials with a high level of neutron self-emission (due mostly to the process of spontaneous fission). Therefore, nuclear terrorists could be very interested in a gun-type nuclear device with reactor-grade or weapons-grade plutonium.

Estimates of the fizzle yield were made by Dr. Carson Mark, former Theoretical Division Leader of Los Alamos National Laboratory.³ He considered "as a purely hypothetical example" a weapons-grade plutonium assembly of the implosion type used at Trinity (the first American nuclear test, July 16, 1945), with the nominal yield of 20 kilotons. The fizzle yield in this case might be 0.5 kiloton. A similar assembly in a gun-type system would produce a fizzle yield of some 10-20 tons.

The fizzle phenomenon is of a statistical nature where the main parameter would be the moment of neutron occurrence during the waiting period. The fizzle could be managed to some extent, but management of this kind requires

some extra technical complications that might be unacceptable for terrorists. Therefore, the “natural” fizzle seems to be more attractive for them. The above-mentioned natural-fizzle yield value of 10-20 tons was estimated for a rather high speed of bringing together two subcritical masses of plutonium (about 300 m/s). A yield about five times lower would be expected at a relative speed of 100 m/s. The corresponding yield value (a few tons) seems to be quite acceptable for terrorists.

Let us assume that the mass of a single plutonium piece would be, say, 5 kg. In this case, its kinetic energy (at a speed of 100 m/s) would be equal to 25 kJ. Such energy may be provided either by high explosives (the explosive energy of TNT is about 4 MJ/kg) or by some source of stored mechanical energy (a compressed spring, for example).

For systems with natural fizzle, the idea of testing makes no sense since every subsequent result can, in principle, differ from the preceding one.

The yield value of few tons is comparable with the explosive energy release in some instances where terrorists used chemical high explosives (as in the Oklahoma City case, for instance). So, a natural question arises, What could be the advantages of a low-yield nuclear device compared to a few-ton blast produced by chemical high explosives? In fact, one could identify certain advantages.

First of all, it would be a direct demonstration of the fact that terrorists do possess a nuclear explosive. From the psychological point of view, this action might produce the most important effect on public opinion.

Second, the nuclear explosion is characterized by higher effective temperatures. This results in a more powerful shockwave and thermal effects. One can estimate the “kill range” of a 2-ton nuclear blast using corresponding scaling laws and reference data about the consequences of the nuclear explosions in Hiroshima and Nagasaki. Such an estimated value will hardly exceed 100 meters.

Third, the nuclear explosion inherently produces radioactive contamination by fission products (not to mention radioactivity induced by fast neutrons). The yield of 2 tons would correspond to total fissioning of only 0.1 gram of plutonium. As a result, about 0.3 Ci of cesium-137 and 0.1 Ci of strontium-90 (the most abundant long-lived fission products) would be generated. The initial activity of short-lived fission products (which decay mostly within a few months after the explosion) would be greater by nearly two orders of magnitude (about 20-30 Ci). Plutonium itself is a toxic material as well, especially in the form of plutonium oxide aerosol, which is produced by a high-temperature blast. This aerosol could disperse over larger distances and be dangerous to the population.⁴

However, these low-yield nuclear devices cannot be “invisible.” It has been shown that neutron emission from an ordinary plutonium warhead can be detected at distances of 50-70 meters.⁵ The corresponding detection range would be two to three times greater for devices using reactor-grade plutonium. It is important to note that the detection range and kill range of a low-yield device are

comparable. This makes it possible to protect some very important targets from terrorist nuclear attacks.

In conclusion, potential nuclear terrorists would encounter no serious technical problems in constructing a simple low-yield (in the order of few tons of TNT equivalent) and low-weight (in the order of a hundred kilograms) gun-type nuclear explosive device using weapons-grade or reactor-grade plutonium. A device of this kind would have destructive and thermal kill ranges of about 100 meters. Moreover, it would produce radioactive fallout with a total intensity of a few tens of curies as well as a cloud containing a few kilograms of plutonium oxide aerosol. The "threshold" amount of plutonium for such a device might exceed to some extent the mass of plutonium for an ordinary nuclear warhead.

This hypothetical example emphasizes the vital importance of very strict control over nonproliferation of any amounts of plutonium (both weapons-grade and reactor-grade material of any isotope composition). It also emphasizes the potential importance of very sensitive neutron detectors.

NOTES

1. Committee on International Security and Arms Control, National Academy of Sciences. 1995. *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*. Washington, D.C.: National Academy Press, p. 44.
2. Cochran, T.B., C.E. Paine. 1995. *Nuclear Weapons Databook: The Role of Hydronuclear Tests and Other Low-Yield Nuclear Explosions and Their Status Under a Comprehensive Test Ban*. New York: Natural Resources Defense Council, p. 6.
3. Mark, J.C. 1993. Explosive properties of reactor-grade plutonium. *Science and Global Security* 4(1):111-124.
4. Fetter, S., F. von Hippel. 1990. The hazard from plutonium dispersal by nuclear-warhead accident. *Science and Global Security* 2(1):21-41.
5. Occasional Report. 1990. The Black Sea Experiment. *Science and Global Security* 1(3-4):323-333.

Problems of Biological Security in Agriculture

*Georgy A. Safonov and Vladimir A. Gavrilov**
Pokrov Biological Preparations Plant

First of all, we would like to say a few words about the Pokrov Biological Preparations Plant. The plant was built in 1978 for two main purposes: (1) producing diagnostic and prophylactic preparations used against especially dangerous diseases, including exotic varieties (all types of foot-and-mouth disease, cattle plague [rinderpest], classical swine fever, Newcastle disease, avian influenza, and others); and (2) stockpiling necessary reserves of biological preparations for use in emergency measures to combat disease. The plant was part of the special system of the USSR Ministry of Agriculture intended for organizing and carrying out efforts to respond to emergency situations arising in the agricultural sphere during outbreaks of especially dangerous diseases. Leading specialists at the plant include scientists working on matters related to eliminating the consequences of unforeseen situations, including biological terrorism.

Over the past decade, the world has seen the exacerbation of the situation between individual countries and groups divided by their various political, territorial, and religious views regarding coexistence: Israel-Palestine, Yugoslavia, Chechnya in Russia. Existing contradictions grew into military confrontations with unpredictable consequences with regard to the methods and means of action used. In fact, we have already seen a case in which the religious sect Aum Shinrikyo carried out a terrorist act using chemical weapons and attempted to initiate production of biological weapons.

In many countries, the public has been concerned about the possible consequences of terrorist acts in our high-tech society, and attempts are being made to develop effective methods of combating these phenomena. A number of sources

* Translated from the Russian by Kelly Robbins.

in the literature provide rather complete coverage of various aspects of the use of pathogens to cause economic, moral, and physical harm to a healthy population.¹

It is generally known that for the majority of countries, agriculture serves as the main source of foodstuffs and raw materials. A sharp reduction in food resources is always accompanied by demoralization and the worsening of demographic indicators regarding the health of the population.

The economic costs involved in fighting epizootic diseases are practically always enormous, not to mention the costs of protecting health and preventing financial damages associated with quarantine measures and reduced labor productivity. One must also consider the additional costs of maintaining personnel to monitor the appearance of infection foci, diagnose animal diseases, quarantine infected individuals, restrict the transport of animals, test the quality of meat and milk, and certify these and other livestock-related products as unfit for sale if necessary. This is a far from complete list of the economic costs borne by the state and counted on by the terrorists. It does not take into account the psychological trauma suffered by farmers and the population as a whole.

Broad-scale movements of people and migrations of animals could serve as the basis for widespread contacts with contaminated food, feed, and water. The population is becoming increasingly mobile (due to tourism and searches for work and new places of residence), while international shipments of animals and livestock-related products are also on the rise. Often, the appropriate safety measures are not taken. Refugees, victims of natural disasters, participants in massive pilgrimages and other religious observances, and individuals temporarily living in crowded conditions represent a favorable target for acts of bioterrorism, especially those involving animal-borne pathogens. In such situations, control and monitoring of animals is usually weakened or completely lacking; therefore, animals in such circumstances can represent a likely source for the transmission of zoonoses.

The destruction of food supplies could be the consequence not only of climatic anomalies, but also of the inadvertent or intentional spread of diseases among animals or plants. For example, practically all the cattle in the Philippines died as a result of a foot-and-mouth disease outbreak in 1917-1927. Outbreaks of foot-and-mouth disease in England (2001) and classical swine fever in Denmark and Holland (1998-1999) not only caused enormous economic losses of more than 3 billion U.S. dollars, but also completely paralyzed economic life in these countries. An outbreak of African swine fever in Cuba (1976) was no less grievous. Another example is the epidemic of Rift Valley fever in Egypt (1977), in which by the most conservative estimates more than 500 people died and another 18,000 became ill in just one year, not to mention the cases suffered by animals.²

The spatial (territorial) or varietal rotation of pathogens always inflicts the heaviest consequences. This can occur not only by means of evolution, but also as a result of the accidental or intentional spread of an active agent.

In recent years, the world community has become increasingly concerned

over the possible use of biological agents in the commission of terrorist acts. History provides no small number of examples in which human corpses, animal carcasses, or infected clothing were used to create micro-outbreaks with the aim of producing major foci of infections. Today, the overwhelming majority of states and their leaders actively oppose the use of pathogens as a means for the mass destruction of people, plants, and animals.

Thanks to the activism of many politicians advocating controls over work with especially dangerous pathogens, you will not hear any strategists of warfare or terrorist acts saying that biological weapons are not only the most economically accessible, but also the most humane of weapons from the standpoint of preserving material valuables or the environment.

The world is still divided into hostile opposing groups based on religious, racial, political, economic, or merely moral-ethical views on coexistence.

It should always be kept in mind that the use of biological agents such as foot-and-mouth disease, cattle plague, African or classical swine fever, avian influenza, or anthrax could initially go unnoticed—and furthermore unprovable—or be explained away as a result of spontaneous external transmission, as has happened on more than one occasion. For example, explanations for the foot-and-mouth disease outbreak in England postulate that it occurred because a restaurant was supplied with infected pork.

But how can one differentiate between happenstance and intention—a terrorist act? This is practically impossible to do. The very fact of an unprovable accusation being made would be an intentional insult to individuals and even states.

The concept of terrorism relative to agriculture seems at first glance to have little applicability, because it is aimed not directly at the physical destruction of people, but only at human food sources. At the same time, we are well aware of the fact that a country left without agricultural resources finds itself in extreme conditions that could lead not only to the removal of a government or change of political course, but also to mass deaths of people due to starvation.

The Chechen conflict has already led to a clearly expressed terrorist action, namely, the bombing of apartment buildings used by the civilian population and subsequent heavy human casualties. The world would not be surprised if tomorrow it heard the news that pathogens had been used in one of the above-mentioned states to destroy not only people, but also animals and crops. However, in this case we would be dealing with an organized action affecting primarily the psyches of the population and government with the aim of changing opinions on a specific issue—territory or independence, for example. In such a case we are fully justified in calling such an action terroristic.

The situation that arose in England with regard to the foot-and-mouth disease outbreak is another matter. At first glance, we see no connection with terrorism. On the other hand, England and surrounding countries have long been free of foot-and-mouth disease. The question is, How and from where did the

foot-and-mouth disease agent arrive in England? It is supposed to have arrived in infected meat, but how did infected meat reach the market? Why was it not discovered by veterinary services in the country of export? And how did it end up in England?

The effectiveness of the international system for monitoring especially dangerous infections largely depends on the responsible attitudes of national veterinary services and governments of UN member countries.

The system for providing notifications of cases of zoonotic disease and quarantine infections is presented in some detail in the reports of an FAO-WHO (Food and Agriculture Organization-World Health Organization) joint expert committee on veterinary sanitation.³ However, in certain cases this system is ignored for reasons of economic constraints, which usually follow after the issuance of official FAO notifications on the presence of quarantine infections in a country. This creates a precedent for the wide-scale spread of especially dangerous infections. We propose viewing such situations of concealment of quarantine disease as a latent form of terrorist action on the part of a state.

A state that has not instituted the appropriate quarantine (intentionally or not, which is another question), not notified other countries in a timely manner, and not taken active measures to recall infected products for heat treatment or other decontamination processing should bear the corresponding responsibility for any consequences.

Bioterrorism can be painstakingly planned and carried out by individuals aware of the consequences of their actions with regard to the chosen target.

In a number of cases, where states in which quarantine infections are present take a passive attitude with regard to preventing the spread of the infectious agent beyond their borders, this should also be viewed as a special form of terrorism that can be termed “latent.” Like intentional terrorism, it can lead to the deaths of people and losses of crops and animals on a massive scale. In this case, such a state—we shall call it a “passive terrorist”—is guilty of spreading pathogens to other territories and is obligated to bear the economic and moral responsibility for the damage caused to the other country, for example, England. In cases of aggressive terrorism, the question must be viewed as a criminal matter in accordance with the existing laws of the country affected.

If in the course of analyzing the causes of an infectious outbreak it can be established and proven that an individual or group is to blame for spreading the pathogen by means of infected food or feed products to another country or to a firm located on the territory of another country, then charges of latent terrorism should be addressed in an international court of law. As for punishment, a decision could be rendered to include not only payment of damages, but also a temporary economic embargo (full or partial) with regard to the guilty country.

The proposed approach and measures for punishment of those to blame for spreading pathogens should reduce the potential threat that such situations will arise.

In addressing possible situations involving the spread of pathogens, we first of all wish to attract attention to the discussion of bioterrorism-related questions by the maximum possible number of scientists and specialists working in the legal field so that in the end, there will be a clear-cut definition of various situations associated with the spread of pathogens.

At a minimum, the following four aspects of the biological threat should be kept in mind:

1. The spread of an agent beyond the borders of states where a particular disease or pathogen is present;
2. The unintentional release of a pathogen from scientific-research or production facilities;
3. The spread of infection by products from infected livestock; and
4. The intentional spread of infection aimed at causing economic pressure or changing the political course of a country.

We have seen dozens of examples in which agents from so-called natural foci infections appeared far beyond the borders of the areas in which they are traditionally found: African swine fever, Venezuelan equine encephalitis, Rift Valley fever, and others.

The territorial rotation of pathogens always causes significant difficulties in the areas where the pathogens have newly arrived. The unexpected appearance of African swine fever in Portugal (1957) and Spain (1957) caused well-founded alarm in many European states. To this day, Portugal and Spain have been unable to rid themselves completely of this uninvited guest.

There are a number of examples of the release of pathogens from institutions or enterprises working with them. For example, during testing of a new foot-and-mouth disease vaccine in 1965, the foot-and-mouth disease virus escaped from the Kursk Biological Plant, causing one of the most severe epizootic outbreaks in the European part of the USSR. It took years to eliminate this outbreak, and the country's economy suffered significant damage.

We are well aware of the fact that industrial or research work with pathogens also requires special safety equipment and technical conditions, depending on their individual properties.⁴

Today in Russia, not only technologies, but also pathogen strains used in production are being sold off. In a number of instances, industrial strains of pathogens differ little from field strains. For example, the majority of technologies for the production of killed vaccines are generally based on field strains of pathogens (foot-and-mouth disease, avian influenza, rabbit hemorrhagic disease, etc.). Furthermore, it seems to us that this technology in no way differs from that used in the production of raw materials for biological weapons. We are certain that one might find no small number of businessmen who, for a relatively small

payment, would sell active raw material without even thinking of the possible consequences of such a deal.

It is commonly known that within Russia, not only are individual people being killed, but entire apartment buildings full of completely innocent people are also being blown up. The Chechnya crisis has not yet passed, and no one can predict the future turn it will take or when it will end.

Furthermore, the entire agricultural sector (including the raising of both livestock and crops) is practically unprotected from terrorism. Foot-and-mouth disease, African and classical swine fever, avian influenza, and anthrax are obviously the most likely and most accessible biological agents for local application against animals.

Highly infectious material can be produced in quantities sufficient for the commission of terrorist acts even in the most primitive conditions—barns, caves, or even animal pens. Doing this would require just 1-2 ml of a pathogen and a susceptible animal. The sick animal could be introduced unnoticed into a large herd, or one might wait for the infected animal to die and then extract highly concentrated material from it (spleen, liver, lungs, etc.), which could then be used to infect feed, pastures, or water supplies or else be sold to the population.

On the territory of the Russian Federation, there are more than 10,000 sites where anthrax spores lie buried. The detonation of any one of these could become a nightmare for the population within a radius of 5-10 km or more.

We would not like to go into detail regarding all possible ways of using biological agents as terrorist weapons, so that this work does not become a textbook for people who have lost their minds for whatever reason.

We have already mentioned the transmission of foot-and-mouth disease from the territory of a biological plant in 1965. Even today, a repeat of such a situation cannot be ruled out, particularly in view of the fact that institutes working with especially dangerous infections are engaged in the production and sale of biological preparations. Furthermore, production discipline has deteriorated significantly during the recent years of economic restructuring. The stream of visitors has grown immeasurably, and protective alarm systems have aged or broken down entirely.

At the same time, many countries are taking a responsible approach to the question of bioterrorism. For example, an international seminar on increasing the level of security for work with dangerous pathogens and other materials was held in October 2000 in the city of Albuquerque, New Mexico. Participants in the seminar included scientists and specialists from the United States, Great Britain, Canada, Sweden, Russia, Ukraine, Kazakhstan, Uzbekistan, and Georgia. The seminar featured discussions of new approaches to the physical protection of institutions working with potentially dangerous materials. Questions regarding the storage, accountability, control, and transport of biologically hazardous materials represented a significant focus of discussion. Personnel-related work was addressed in detail, including the hiring of personnel for re-

sponsible positions, reliability, professional skill, and readiness to work in emergency situations. Several potential situations that might arise at facilities were reviewed:

- The theft of biomaterials for the purpose of committing acts of terrorism or blackmail;
- Terrorist acts aimed at disrupting the functions of production facilities or premises housing security personnel; and
- Incursion onto the territory of a facility in the aim of committing illegal acts and other situations.

Illegal actions could be committed not only by terrorists or criminals, but also by disgruntled or bribed employees or even representatives of animal rights groups. In this regard, any system for protecting dangerous facilities must feature multiple levels of security: a reinforced concrete wall with two alarmed perimeters and video surveillance. Each critical building, floor, material storage room, and container of biomaterials must be equipped with an alarm system.

In conclusion, we feel it is necessary to discuss the most important problem from our point of view, that of the bioprotection of agriculture. First, legislative limits must be placed on the number of scientific institutes and biological enterprises that are authorized to work with especially dangerous pathogens and with infectious materials in general. The international community must develop methods for monitoring the safe operation of biological enterprises regardless of their ownership. State agencies must bear responsibility for ensuring compliance with international safety standards for the operation of biological enterprises. They bear this responsibility not only to their own countries, but to the world community in general.

Of course, the most complex aspect of this problem involves the effectiveness of control, especially internationally or bilaterally. In this regard, concrete steps are already being taken in Geneva to create an agreement on a mechanism for such control. We believe that resolving the question of effective control over biosecurity will be possible only after normal partner relations are established between countries, peoples, and first of all, state structures.

The difficulties of biocontrol can be overcome only as a result of procedurally unrestricted exchange visits and contacts between scientists and production personnel and their colleagues abroad. One should not follow the thesis that private firms cannot be controlled by international agencies. In visiting other countries, we have always been surprised by such a convenient method of limiting access to this or that firm. Our colleagues also probably find it hard to understand when they are restricted from visiting facilities. How can we speak of any sort of trust here? Fear over so-called industrial secrets cannot be the reason for refusing access. Citizens of any country must be subject to the laws of their own country, as well as to international laws. If not, neither mutual trust nor

appropriately effective control will ever exist. Disagreements over issues concerning exchanges of visits could become a basis not only for mistrust, but also for political blackmail.

It is also essential to strengthen the 1972 convention on the prohibition of biological weapons, first of all by creating an atmosphere of international trust.

From the first years of its production activity, the Pokrov Biological Preparations Plant of the USSR Ministry of Agriculture operated on a self-financing basis, requiring no budget support from the government. This was made possible not only by the plant's large-scale production of vaccines against practically all viral infections existent in the Soviet Union, but also by centralized state orders for the production and stockpiling of reserves of vaccines for foot-and-mouth disease, cattle plague, classical swine fever, Newcastle disease, sheep pox, and avian pox.

The plant is a potentially dangerous enterprise with regard to the livestock industry. The range of viral infectious agents with which the Pokrov Biological Preparations Plant worked, as well as the location of the plant in a region with many livestock farms and enterprises, determined the need for a special closed operating regime. Admission to the plant required showing a badge or pass, visits were restricted, and a security system was in place around the perimeter of the plant. Indeed, the size of the area occupied by the plant and the special construction characteristics of several earthquake-resistant buildings on the site attract heightened interest regarding the nature of work being carried out there.

The plant produced more than 40 biological preparations, the lion's share of which were unique, patented products. This made it possible for the plant to produce biological preparations worth 50 million dollars or more each year. The collapse of the Russian economy in the transitional period led to a significant reduction in livestock numbers and a sharp drop in demand for biological preparations. Today the output volume at the plant totals 10 percent of capacity. The high energy demands of the production process have become a sort of Achilles' heel with regard to the profitability of products manufactured in small volumes. In connection with this problem, the plant is experiencing a critical period. A significant portion of the employees have moved on to other jobs in private firms. The plant currently employs more than 700 people, 150 of whom are scientists or specialists with a higher education.

In the aim of increasing the profitability of production and improving its financial position, the plant plans to carry out a substantial modernization and reconstruction project. This will involve reducing energy costs in the production shops by dismantling the centralized refrigeration and compressed air systems and replacing them with small localized units in each individual shop. More than 20 fermenters will be dismantled in order to retool the shops to manufacture pharmaceutical products. In the space freed up after removal of the fermenters, plans call for installing production lines for liniments, medicine tablets, and intravenous solutions.

The production of veterinary probiotics and immunomodulators is also to be established in the buildings to be freed up after the renovations. Equipment for feed production and quality control will be installed in the decrepit older buildings, along with a storage facility for animal embryos. With financial support from partners, plans will be carried out to establish a poultry farm processing and storage facility with a capacity of 2 million eggs per year.

A number of research and implementation projects have recently been developed in cooperation with the International Science and Technology Center (ISTC) and the Defense Threat Reduction Agency. Implementation of these projects will facilitate the reconstruction of the plant's production capacities and the reduction of tensions regarding issues of mutual trust and site visits.

Completion of the entire range of planned reconstruction projects at the plant will make it possible to convince the public of the peaceful nature of our production facility. The planned long-term strategic cooperation with a number of U.S. organizations will also promote an improved political atmosphere between our countries. Moreover, the plant hopes to make a concrete contribution to the prevention of especially dangerous infections not only within Russia, but also in other countries. We are convinced that international cooperation on the issue of biological security will promote collaboration among scientists of various countries in preventing other types of terrorism.

In accordance with the Initiatives for Proliferation Prevention (IPP) Program, the plant will be able to cooperate with the United States Industry Coalition (USIC) and the European Union programs INTAS, Tacis, and others. The financial support provided by ISTC in the form of grants makes it possible to host foreign colleagues at the plant and openly show our production capabilities, which will reduce concerns with regard to hidden or closed facilities.

We have always taken a serious approach to critical comments from the international commission that visited the plant in 1993 regarding its concerns about the plant's technical capabilities. We believe that international cooperation will enable us to remove these worries on the part of the public.

Even today, a potential danger exists regarding the appearance and spread of panzootic outbreaks of such infections as monkeypox, Marburg disease, Ebola, prion encephalopathies, foot-and-mouth disease, African and classical swine fever, and others. These infections have really appeared on the horizon of the twenty-first century in connection with the growth of international trade, tourism, ethnic conflicts, natural and technological catastrophes, and an ever-increasing number of militarized conflicts.

Given the real threat of biocatastrophes, efforts must be stepped up to create international institutions that will focus their activities on rendering practical assistance to states in eliminating even small foci of especially dangerous exotic diseases. First of all, the WHO and FAO must resolve the problem of creating emergency stockpiles of preventive and curative medicines for dealing with wide-scale infectious outbreaks. Consideration must also be given to questions of

strategy and tactics in combating such outbreaks, including universal slaughter, the destruction of infected animal carcasses, and comprehensive vaccination campaigns in the event that a localized outbreak becomes epizootic.

Let us wish for all of us a strong sense of responsibility not only for the fate of our own peoples, but also for that of our beautiful planet Earth. Let us not forget the opinions of our cosmonauts—that Earth as a cosmic body is but an infinitely small speck of dust in the limitless ocean of the universe. The natural harmony of living nature on Earth has continued for many millions of years, but today life on Earth depends on the reason and will of mankind, including all of us here.

NOTES

1. Rozbern, T., E. Kabat. 1955. *Bacteriological War*. Moscow: Voenizdat.
 Rotshild, D. 1966. *Tomorrow's Weapons*. Moscow: Voenizdat.
 Sokolov, G.A. 1968. Thermonuclear, chemical, and biological weapons: means of mass destruction. *Mendeleev Chemistry Journal*.
 Timakov, V., F. Koroshkov. 1969. Protecting people from the threat of chemical and bacteriological war. *Medical Newspaper*.
 Thant, U. 1970. *Chemical and Bacteriological (Biological) Weapons and the Consequences of Their Use*. Report of the UN Secretary General at the 25th Session of the UN General Assembly.
 Baroyan, O.V. 1971. *The Fate of Conventional Diseases*. Moscow: Meditsina.
 Georgievsky, A.S., O.K. Gavrilov. 1975. *Social Hygiene Problems and Consequences of War*. Moscow: Meditsina.
 FAO-WHO. 1975. *The Veterinary Contribution to Public Health Practice*. Technical Report Series No. 573. Geneva.
2. FAO-WHO. 1982. *Bacterial and Viral Zoonoses*. Technical Report Series No. 682. Geneva.
3. FAO-WHO. 1982. *Bacterial and Viral Zoonoses*. Technical Report Series No. 682. Geneva; WHO. 1985. *Laboratory Biosafety Manual*. Geneva.
4. WHO. 1985. *Laboratory Biosafety Manual*. Geneva; Drozdov, S.G., N.S. Garin, L.S. Dzhindonyan, V.M. Tarasenko. 1987. *Fundamentals of Safety Equipment in Microbiological and Virological Laboratories*. Moscow: Meditsina.

International Centers as a Basis for Controlling Infectious Disease and Countering Bioterrorism

Lev S. Sandakhchiev, Sergey V. Netesov, Raisa A. Martynyuk*
Vector State Research Center for Virology and Biotechnology
Russian Federation Ministry of Health

The task of our panel is to examine the role of international collaboration in countering terrorism. In my presentation, I would like to address the need for international cooperation in combating bioterrorism.

During the past decade, policy makers and military and civilian experts have shown more and more interest in the bioterrorism issue. Much discussion and analysis has centered on possible biological agents of viral or bacterial etiology, scenarios of how to prevent and respond to the use of these agents, and epidemic response capabilities in terms of the availability of competent personnel and diagnostic and therapeutic products.

As a rule, the scenarios of bioterrorism incidents are far from optimistic in terms of both human casualties and costs associated with containing the direct consequences of such actions, not to mention the resulting economic breakdown in the region affected and the lasting psychological effect on the population.¹

Terrorism is now a growth industry, and the possibility of a chemical or bioterrorist attack is increasingly defined as “not if, but when.” However, even the United States, which has longstanding experience in infectious disease control worldwide, developed its response plan, *Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response*, only in the year 2000.² This plan, which involves coordinated response to and elimination of such events by more than 10 agencies, is focused on five major areas:

- Preparedness and prevention,
- Detection and surveillance,

* Deceased.

- Diagnosis and characterization of biological and chemical agents,
- Response, and
- Communication.

Included in all of these areas are proposals for personnel training as well as investigation of and total preparedness for detection and elimination of consequences of possible attacks using chemical or biological agents in all states and cities. The key point is to design a multilevel laboratory network to efficiently warn public health authorities at the community, state, district, and city levels if biological and chemical agents are detected. This plan is aimed at significantly reengineering the existing infrastructure for infectious disease response and control.

I would like to especially emphasize certain features that differentiate bioterrorism from other kinds of terrorism.³ Explosive substances are fairly widespread and not very diverse. Chemical agents that could be used for terrorist purposes are well studied as potential chemical weapons, and detection procedures have been developed for many of them, along with measures for the treatment and decontamination of those affected. In case of biological agents, however, it is an absolutely different situation. In nature, there are a great variety of viruses, bacteria, and fungi that cause diseases in humans, animals, or plants. Experts estimate that currently we are aware of far less than one percent of existing viruses and several percent of microbes. Nature is continuously creating new pathogens, the so-called emerging infections, and this potential is simply inexhaustible. During the last 20 years alone, scientists have discovered more than 30 new infectious agents (e.g., HIV, Marburg, and Ebola viruses) against which neither cures nor preventive drugs are yet available.

As a result of their ability to change, known diseases such as influenza, tuberculosis, malaria, and some others can relatively easily overcome conventional immunization and drug-based approaches to prevention and therapy.

Humankind has been fighting a biological war against microbes since its emergence, and even now infectious diseases account for almost 30 percent of worldwide mortality. Although experts on biological weapons and bioterrorism often operate with a limited list of several dozen infectious agents, we should not underestimate the possible terrorist use of any of the diverse pathogens existing in nature.

Thus, the task of establishing a global system of surveillance for possible natural or artificial outbreaks is far more difficult than for chemical agents or explosives.

It is important to realize that biological agents act over time and have a latent period during which the carrier of infection may find herself or himself in another city or even another country, where the outbreak of disease may be actually identified. It may take much time to prove the bioterrorist use of microorganisms since it will require a comprehensive epidemiological analysis (e.g., investigation of all stages involved in the manufacture and distribution of food-

stuffs, in the case of food poisoning). The well-known case of the terrorist use of *Salmonella* in a salad bar in Oregon in 1984 resulted in sickening more than 700 individuals. However, it was initially regarded as a natural outbreak, and only one year later it was proven that *Salmonella* had been used by religious cult extremists to prevent voting in Oregon. By the way, the U.S. public learned about that case many years after it occurred.

Therefore, it is medical personnel that are the first to have to deal with biological incidents, and it is public health capabilities that determine the preparedness of a country, region, or city for timely detection and elimination of consequences of the use of biological agents. For this reason, financial and organizational efforts should be focused on civilian rather than military agencies.

The nation must be prepared to deal with the detection and elimination of consequences of outbreaks caused by any biological agent, including both conventional and exotic species of microorganisms. The existing systems for nationwide epidemiological surveillance and control of infectious diseases should be capable of identifying, containing, and eliminating an infectious disease outbreak regardless of whether it is the result of the natural manifestation of a pathogen or its deliberate use.

All these features require that international collaboration be established in order to set up a system of efficient alert and response. This issue was specifically addressed at the May 2001 54th World Health Assembly in the report by the Secretariat entitled "Global Health Security—Epidemic Alert and Response." It was noted that in 1995 the World Health Assembly adopted resolutions WHA48.13 on new, emerging, and reemerging infectious diseases and WHA48.7 on the revision and updating of the International Health Regulations. The World Health Organization (WHO) totally realized the need for enhancing epidemiological and laboratory surveillance at the national level as "the main defense against the international spread of communicable diseases."

Increased population movements (through tourism or migration or as a result of natural or technologic disasters or conflicts), growth in international trade in food and biological products, social and environmental changes associated with urbanization, and changes in food processing technologies, food distribution networks, and consumer habits determine the likelihood that an infectious disease will emerge in a given country and so create a real threat to the remaining countries worldwide.

The Secretariat pointed out the increased possibility of the intentional use of infectious disease agents and emphasized that natural epidemics and those due to the deliberate use of biological agents may manifest themselves in the same manner. The Secretariat also noted that the need for international cooperation on this issue appears far more important now than when this idea was discussed at the first International Sanitary Conference in 1851. Such cooperation has been maintained by WHO since its establishment in 1948.

In 1997, WHO established a special system to seek, collect, and verify in-

formation on reported outbreaks. Based on the close cooperation of WHO Collaborating Centers with governmental and nongovernmental agencies, the system provides information on confirmed disease outbreaks on the WHO web site (www.who.int/disease-outbreak-news) and in the WHO *Weekly Epidemiological Record* (www.who.int/wer). At global level, laboratory networking takes place (www.who.int/emc), focusing on such infections as hemorrhagic fevers (including Ebola virus) and poliovirus. Efforts are also devoted to preparation of databases such as the WHO antimicrobial resistance data bank (ARInfoBank) (www.who.int/emc/amr.html), influenza FluNet (<http://oms2.b3e.jussieu.fr/flu-net/>), rabies RabNet (www.who.int/emc/diseases/zoo/rabies.html), and others. WHO has called on its member states to establish partnerships to involve both civilian public health and military medical capabilities.

WHO continuously draws the attention of its member states to the ultimate role of national potential in ensuring the epidemiological welfare of other countries, so it plans to expand national training programs in intervention epidemiology worldwide as well as the Training in Epidemiology and Public Health Interventions Network (TEPHINET). Major conclusions based on discussions of the Secretariat report were reflected in Resolution WHA54.14 entitled "Global Health Security: Epidemic Alert and Response" (http://www.who.int/wha-1998/EB_WHA/PDF/WHA54/ea54r14.pdf). A good example that deserves serious attention and similar action is the establishment of the WHO Bureau in Lyon (France) as a model for using national potential to contribute to the training of personnel for countries at high epidemic risk (www.who.int/emc/lyon).

At the global level, huge resources are already available to combat infectious diseases. Certainly, these will also be used to counter bioterrorism incidents.⁴ They include hundreds of WHO Collaborating Centers worldwide specializing in certain infections; a Pan-American Health Organization (PAHO) laboratory network; the International Clinical Epidemiology Network (INCLIN); the Pasteur Institutes network; an international research centers network of the National Institutes of Health (NIH) that involves many universities across the United States; and the Centers for Disease Control and Prevention (CDC) offices in numerous countries, many of which conduct epidemiological surveillance and provide field epidemiology training for different regions. The U.S. Army and Navy have also established a specialized network of research centers in several countries. It should be noted that this particular resource is very much focused on specific tasks and, except for the Epidemiologic Intelligence Service (EIS) centers, is not oriented toward detection and identification of the entire pathogen range.

As a matter of fact, to localize and contain unusual outbreaks posing a threat to global public health, WHO has set up task forces to be deployed during such outbreaks. A number of epidemics have been eliminated in this way in recent years, although this has required tremendous efforts in terms of coordination, material supply, transportation, communication activities, and so forth.

Another approach was proposed by the outstanding epidemiologist Dr. D. A. Henderson,⁵ who, based on many years of experience as a leader and actual participant in the global smallpox eradication program, arrived at the conclusion that fixed-site international centers should be established in 15 regions of the world. These should include the following:

- Inpatient and outpatient capabilities to deal with infectious diseases;
- Research and diagnostic laboratories;
- Epidemiological teams to function like the EIS to cover regions with populations of 2 million to 5 million; and
- Education and training capabilities to provide training to national and international personnel.

Systematic studies of a specific region make it possible to obtain invaluable databases, investigate different factors that can influence the epidemiological situation, and identify unusual cases requiring careful examination.

According to Henderson, this network of regional centers should involve collaboration with such organizations as CDC, the National Institute of Allergy and Infectious Diseases (NIAID), and academic research centers. To provide stability and a legal framework, they should work closely with WHO and government authorities in the countries where they would operate.

The leader of the U.S. Emergency Interagency Working Group, Jewellyn J. Legster, evaluates Dr. Henderson's proposal very highly, though the former believes that prior to realizing this idea it is necessary to work to analyze existing regional capabilities and choose geographic regions at high epidemic risk. Such regional centers should also have research programs in epidemiology and the region's key problems in terms of infectious diseases, diagnostic, and therapeutic means, as well as personnel training.⁵

As a follow-up to the U.S. Institute of Medicine recommendations, the WHO Department of Communicable Disease Surveillance and Response together with the International Center of Genetic Engineering and Biotechnology (ICGEB) and several nongovernmental organizations (Program for Appropriate Technology in Health [PATH], INCLIN, and TEPHINET, the so-called Alliance against Infectious Diseases) prepared a program proposal in 2000 entitled "Global Monitoring, Research and Training to Control Infectious Diseases."

In the initial stage of the program, 10-12 laboratories or institutes would be identified in strategically important regions at high epidemic risk and with insufficient surveillance capabilities. Those laboratories should have laboratory and clinical study capabilities and a potential for conducting epidemiology work, access to air and ground transport, possibility of telecommunications installation, and prospects for future expansion.

Centers thus identified would have status as WHO Collaborating Centers and preferred access to WHO programs and those of Health Ministries in WHO

member states. They would be coordinated by the WHO Office of the Strategic Alliance.

Each center would in turn be established by taking into account the region's specific needs and, in the initial stage, would be provided with the necessary resources to create the most advanced potential for diagnostic, clinical, and epidemiological activities. It also would be provided with telecommunications equipment to be able to communicate with the other centers, as well as with regional, federal, and international agencies involved in infectious disease surveillance and response.

Each center would establish regional networks to include clinics, institutes, education establishments, and others, and it would participate intensively in the region's infectious disease programs. The regional network would involve enterprises manufacturing specialized pharmaceutical products that, through technology transfer, would be given an opportunity to meet the region's needs for standard diagnostic tests and therapeutic products.

The regional network should also involve research laboratories that develop diagnostic and therapeutic products and vaccines, as well as biosafety research laboratories studying the safety of biological substances and microorganisms to humans and the environment.

The program envisages that within 8-10 years, a worldwide network of regional centers would be up and running, and thus a long-term sustainable regional potential for communicable disease control would be created. It is proposed that some of these centers would become centers of excellence like CDC, NIAID, and ICGEB.

The authors note that the proposed approach would represent the most reliable way of preventing and dealing with possible future pandemics (for more information, send a message to WHO at allaid@who.int).

In the above WHO Secretariat report, it was noted that possible mechanisms to support the initiatives to enhance epidemiological surveillance may be based on Article X of the 1972 Biological and Toxin Weapons (BTW) Convention. This article seeks to enhance international cooperation on the peaceful use of biological material, equipment, and technologies. Within the measures envisaged, state parties would receive assistance in strengthening their potential in infectious disease surveillance and response, including research and development activities.

Therefore, it is crucial that the above-mentioned international institutions not only provide the region's epidemiological protection in case of natural or terrorist events using microorganisms, but also contribute to efforts in the extremely difficult political task of confidence building, which is an important factor in enhancing the 1972 BTW Convention.

For many years, our institute—Vector State Research Center for Virology and Biotechnology of the Russian Federation Ministry of Health—has been involved in combating viral infectious diseases. In recent years we have been

discussing the prospects for reorganizing the institute into a regional center similar to those described above.

The institute was established in 1974 with the task of conducting basic and applied research on extremely pathogenic viral agents such as the less-studied Marburg, Ebola, Lassa, and other viruses related to potential biological weapons (BW) agents. The research was aimed at assessing the potential threat posed by these agents and developing means for their diagnostics, prevention, and therapy. Maximum biological containment laboratory facilities and clinical and epidemiological capabilities were built, in addition to the standard engineering infrastructure and a set of scientific and supporting facilities, including a laboratory animal breeding and holding facility. The total area of existing buildings and facilities amounts to 250,000 square meters.

Before 1992, Vector received all of its funding from the federal budget and was just beginning to establish manufacturing activities. Access to workplaces by and communication with foreign scientists were limited. The same limitations applied to the participation of Vector scientists in international conferences and the publication of scientific papers.

In 1989, it became obvious that Vector should be restructured⁶ to adapt to changing economic conditions that ultimately resulted in a significant cutback of federal budget funding. A program was prepared for Vector's long-range development, with the focus on conducting much more public health and veterinary medical research on infectious diseases such as HIV/AIDS, tick-borne encephalitis, viral hepatitis A and B, measles, and others. This would include development of diagnostic tests, vaccines, and antivirals as well as establishment of manufacturing facilities for diagnostic, therapeutic, and prophylactic products.

In 1993, Vector became a State Research Center and started to receive federal budget funding to support its R&D activities through government civilian programs. The development of pharmaceutical manufacturing activities was supported by government investments and credits, which allowed us to renovate and upgrade several facilities and purchase necessary equipment.

Currently Vector is a scientific center consisting of six scientific research institutes and three daughter companies manufacturing a broad range of products. We have managed to retain most of our key scientific personnel and establish sustainable manufacturing activities. During recent years, Vector's income pattern has changed dramatically. While in 1990 78 percent of funds came from the federal budget, in 2000, 77 percent of total income came from product sales.

I would like to say a few words about the role of international foundations and organizations in Vector's reorientation toward public health and agriculture-oriented programs.

In 1992, the International Science and Technology Center (ISTC) was established as a nonproliferation-targeted program for the Newly Independent States (NIS). The same goal was set for the U.S. Civilian Research and Development Foundation (CRDF), which was established by the National Science Foun-

dation in 1995, and for the Newly Independent States Industrial Partnering Program (IPP, currently known as Initiatives for Proliferation Prevention), which is operated through the U.S. Department of Energy with the involvement of the United States Industry Coalition (USIC). Collaboration with the European Union programs INTAS, Tacis, and others is opening up big opportunities.

During 1995-2000, we completed 29 projects with these organizations. Today, we have 26 active projects, including 23 ISTC-funded projects. In 1998, these projects began to play a significant role in Vector's budget, whereas the contribution they made amounted to 30 percent of funds provided from the Russian federal budget. In 2000, the funding under these programs had grown to almost twice as much as the funding provided from the Russian federal budget, and this year the amount of funding under project agreements that have been concluded is approximately \$10 million.

Grant funding and a transparent character of work allow us to receive our foreign colleagues and, in turn, travel ourselves to get acquainted with foreign laboratories. Vector employees have attended dozens of international conferences and workshops. Hundreds of our scientists have visited their foreign counterparts on-site. This has made it possible to create an atmosphere of openness and transparency at Vector, which is critical to science and scientists. Thanks to support provided for our scientific staff, we have been able to maintain our relationships with NIS scientists and scientists from other regions in Russia.

Our employees attend international refresher courses, including English language training, patent and R&D commercialization classes, and training programs in good laboratory, manufacturing, and clinical practices. These activities helped us realize that without implementing international quality standards in science and production, we could hardly hope that our R&D products would be competitive on the world market.

Thanks to grant funding, our scientists are able to conduct research using up-to-date equipment and supplies as well as the latest techniques to gain world class results. I would especially like to mention the Biotechnology Engagement Program (BTEP) of the U.S. Department of Health and Human Services (DHHS). BTEP involves the study of infections such as HIV/AIDS that represent serious public health problems, field epidemiology of hemorrhagic fevers, (multi-) drug-resistant forms of tuberculosis, and research on hepatitis, measles, and variola viruses under an international program under the aegis of WHO. At Vector, we have one of the two WHO Collaborating Centers on smallpox (the other is at CDC, Atlanta), and we collaborate with WHO and our U.S. colleagues on a regular basis on this important program. The study of this infection is of special importance to current efforts to counter the bioterrorism threat.

Very focused efforts are also being planned and implemented under the Defense Threat Reduction Agency (DTRA) Cooperative Threat Reduction (CTR) program with regard to bringing physical security and biological safety systems at the maximum biocontainment facilities at Vector up to the highest modern

standards. Serious efforts are being undertaken to bring laboratory work with research animals and pharmaceutical manufacture at Vector's daughter enterprises up to GLP and GMP standards, respectively.

We take very seriously the criticisms concerning the alleged use of U.S. government funds by Russian institutes for whatever prohibited purposes. These concerns have been voiced in the recent study prepared by the U.S. General Accounting Office and a study conducted by the Henry L. Stimson Center, and others.⁷

Despite the lack of evidentiary support for these statements, we should admit that it could change the situation in principle if the recipient institution were operating on an international regimen ensuring confidence and transparency. For several years, we have been discussing this problem with representatives of the U.S. State Department, DTRA, DHHS, and Russian authorities, as well as with the scientific community at several international conferences.⁸ We are now in the process of discussing with DHHS experts a BTEP-ISTC project entitled "Development of Concept of an International Center for the Study of Emerging and Re-emerging Infectious Diseases." This project proposes to define in greater detail the ways in which the above-mentioned approaches could be implemented.

By an "International Center," we mean an international organization established by an intergovernmental agreement, similar to those of ISTC or the Joint Institute for Nuclear Research in Dubna, the European Organization for Nuclear Research (CERN) in Switzerland, or the International Center for Genetic Engineering and Biotechnology in Trieste (Italy). Nonproliferation and threat reduction goals can be achieved only through transparency and confidence building when the International Center is established and operated with free access to the program and results obtained, and with free access to financial information and to all facilities and all staff of the center. Continuous involvement of foreign scientists in work at this center would be a powerful instrument of confidence building.

Although the process of establishing the International Center is complex and may take several years to complete, the proposed arrangement would provide for a long-term strategic collaboration, which is far less subject to political or economic fluctuations in member states. International partnership would accelerate the study of dangerous pathogens and the development of state-of-the-art public health products for diagnosis, prophylaxis, and therapy, as well as integration of our institution into the WHO international infectious disease control network proposed by the Strategic Alliance Initiative.

The establishment of the proposed International Center would allow us to join our efforts to counter bioterrorism. It is, however, important to establish an appropriate regimen for the use of infectious agents and scientific results obtained to avoid their possible misuse for illicit purposes.

I take this opportunity to emphasize the key role played by the staff of the Russian Federation Ministry of Industry, Science, and Technologies; the Russian

Federation Ministry of Health; RAO BIOPREPARAT; the Russian Academy of Sciences; the Russian Academy of Medical Sciences; the Institute of International Security of the Russian Academy of Sciences; the U.S. Department of State; ISTC; DTRA-CTR; the U.S. Department of Energy; DHHS; CDC; NIH; the U.S. National Academy of Sciences; USDA; and CRDF in the development of international collaborations at Vector.

ACKNOWLEDGMENTS

I wish to thank Mr. V.V. Ryabenko and Mr. A.V. Mironov for their help in editing this presentation.

NOTES

1. Preston, R. 1998. The bioweaponers. *The New Yorker* (March 9): 52-65.
- Preston, R. 1998. Bio-warfare: fiction and reality. *Genetic Engineering News* (March 1): 6-39.
2. Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response Recommendations of the CDC Strategic Planning Workgroup. April 21, 2000 / 49(RR04): 1-14.
3. Committee on R&D Needs for Improving Civilian Medical Response to Chemical and Biological Terrorism Incidents. Health Science Policy Program. Institute of Medicine and Board on Environmental Studies and Toxicology. Commission on Life Sciences. National Research Council. 1999. Chemical and Biological Terrorism. Research and Development to Improve Civilian Medical Response. Washington, D.C.: National Academy Press.
- Proceedings of the Eleventh Amaldi Conference on Problems of Global Security. 1999. (Moscow, November 18-20, 1998). Moscow: Nauka.
4. Lederberg, J., R.E. Shope, S.C. Daks, Jr., eds. 1992. *Emerging Infections: Microbiological Threats to Health in the United States*. Washington, D.C.: National Academy Press.
5. Morse, S.S., ed. 1993. *Emerging Viruses*. New York: Oxford University Press.
6. General Accounting Office. 2000. Biological Weapons: Effort to Reduce Former Soviet Threat Offers Benefits, Poses New Risks. Report [NSIAD-00-138].
7. General Accounting Office. 2000. Biological Weapons: Effort to Reduce Former Soviet Threat Offers Benefits, Poses New Risks. Report [NSIAD-00-138].
- Chemical and Biological Weapons Nonproliferation Project. 1999. Stimson Center Report No. 32. Toxic Archipelago. Preventing Proliferation from the Former Soviet Chemical and Biological Weapons Complexes. Available on-line at <http://www.stimson.org>.
8. Sandakhchiev, L.S., S.V. Netesov. 2001. Strengthening the BTWC through R&D restructuring: the case of the State Research Center of Virology and Biotechnology "Vector." *The Role of Biotechnology in Countering BTW Agents*. Amsterdam: Kluwer Academic Publishers; Netesov, S.V., L.S. Sandakhchiev. 1999. The development of a network of international centers to combat infectious diseases and bioterrorism threats. *ASA Newsletter* 70 (February 19): 2-6; Sandakhchiev, L.S. 1998. The need for international cooperation to provide transparency and to strengthen the BTWC. In *Conversion of Former BTW Facilities*. E. Geissler et al., eds. Amsterdam: Kluwer Academic Publishers, pp. 149-156.

The Role of Internal Affairs Agencies in Efforts to Fight Terrorism Under High-Technology Conditions

*Oleg A. Stepanov**

Academy of Administration, Russian Ministry of Internal Affairs

The problem of the role of internal affairs agencies in the life of society and the state today is insufficiently developed inasmuch as there is currently no generally accepted understanding of the concept of “internal affairs agencies.” In the draft law “On Internal Affairs Agencies,” the author of the bill provides the following definition: “Internal affairs agencies represent a system of state agencies of the Russian Federation that take countermeasures against illegal activities and ensure public and individual security on the basis of provisions of the Constitution of the Russian Federation and principles and norms of international law.”

With this definition in mind, we may turn to one of the most complex aspects of the activities of internal affairs agencies, namely, that connected with the problem of combating terrorism under conditions characterized by the development of information-based high technologies. Within the scope of this problem, two pressing questions may be highlighted. The first concerns legal conditions for countering high-tech-oriented manifestations of terrorism. The second involves facilitation of the scientific-technical development of the country’s population in a way that is proper from a legal standpoint.

In considering these questions, it should be noted that in Moscow alone in 1999-2000, five cases of successful attacks against very important information resources and potentially hazardous industries were detected and revealed. Meanwhile, the existing procedural and criminal legislation as well as the laws “On the Militia” and “On Operational Search Activities” do not allow for effective countermeasures against this phenomenon. Given conditions in the information-

* Translated from the Russian by Kelly Robbins.

based society, the text of at least six articles in the current Criminal-Procedural Code of the Russian Federation should be changed to ensure that the rights of citizens are guaranteed. Specifically, these include Articles 12, 69, 83, 84, 170, and 174.

It is proposed that Part 2 of Article 12, “Sanctity of the Home, the Protection of Personal Life, and Confidentiality of Correspondence,” be amended as follows: “The personal lives of citizens and the confidentiality of correspondence, telephone conversations, and telegraph messages are protected by law. Citizens do not have the right to use communications channels, including telecommunications systems channels, for illegal purposes.” The existing text would continue from there.

It is proposed that Part 1 of Article 69 be amended as follows: “Any factual data, including information stored by machine, computer, or computer system or network, may be used as evidence in a criminal case. On the basis of this information, organs of inquiry, investigators, and courts by legally-established procedures establish the existence or absence of socially dangerous actions and the guilt of the individual who took such action and make determinations on other circumstances having significance for the correct resolution of the case.” The existing text would continue from there.

Article 83, “Material Evidence,” should be amended as follows: “Material evidence is defined as objects that have served as tools of a crime, have retained traces of a crime, or have been the objects of the criminal activities of the accused, such as money and other valuables earned by criminal means as well as information stored by machine, computer, or computer system or network. Material evidence also includes all other items, including printouts of computer systems or network operation logs, that could serve as the means for uncovering a crime, establishing the factual circumstances of the case, or revealing the guilty, either in proving the truth of the accusation or in mitigating responsibility.”

It is proposed that Part 1 of Article 84, “The Protection of Material Evidence,” be amended as follows: “Material evidence must be described in detail in the inspection protocols and photographed if possible, or else transferred to information storage media (paper, machine-based, etc.) in a way that precludes the loss, intentional destruction, or modification of the information, including that taken from computers and computer systems and networks. This information shall be placed in the case file by special order of the individual conducting the inquiry, investigator, or prosecutor or by determination of the court. Material evidence must be preserved during the course of the criminal case.” The existing text would continue from there.

It is proposed that Parts 2 and 3 of Article 170, “Procedures for Conducting Seizures and Searches,” be amended as follows: “In making a seizure, after presenting the order the investigator requests that the items and documents subject to removal, including information stored by machine, computer, and com-

puter systems and networks, be handed over. In the event this request is refused, he makes a forced seizure.

“In conducting a search, after presenting the order the investigator requests that the tools of the crime, items and valuables obtained by criminal means, and any other items or documents having possible significance to the case, including information stored by machine, computer, and computer systems and networks, be handed over. If they are handed over voluntarily, and there are no grounds for suspecting concealment of the target items, documents, and information stored by machine, computer, and computer systems and networks, the investigator has the right to limit himself to taking the items handed over and not making further searches.” The existing text would continue from there.

Part 2 of Article 174, “The Seizure of Postal and Telegraphic Correspondence,” should be amended as follows: “When it is necessary to intercept correspondence for the purpose of its review and seizure, the investigator shall submit an order providing justification. After authorization of the above order by the prosecutor or judge, the investigator forwards the order to the appropriate postal or telegraphic institution or to the organizations providing telecommunications services. He requests that correspondence be intercepted and provides information on the time of his arrival to review and seize the intercepted correspondence. The review and seizure are conducted in the presence of witnesses selected from among staff members at the postal-telegraphic institution or organization providing telecommunications services. The investigator has the right to call on the assistance of an appropriate specialist to participate when necessary in carrying out the seizure of postal or telegraphic correspondence or information from the electronic mail system.” The existing text would continue from there.

Institution of all the above-proposed changes would facilitate the creation of a mechanism by which internal affairs agencies could combat acts of high-tech terrorism.

In this regard, it is important to focus attention on the need to make corresponding changes and additions in Articles 78 (Evidence), 85 (Material Evidence), 86 (Storage of Material Evidence), 185 (Procedures for Conducting Searches and Seizures), and 188 (Interception, Review, and Seizure of Postal and Telegraphic Correspondence) of the draft of the new Criminal-Procedural Code of the Russian Federation, which is currently being developed by the Legislation Committee of the State Duma of the Russian Federation.

In addition to the items noted above, a Part 8 with the following wording should also be added to Article 5 of the Federal Law “On the Militia:” “The storage of personal data in electronic form, as well as the giving of instructions to militia personnel to conduct automated processing of name-identified data, is carried out according to procedures established by legislation of the Russian Federation.”

From the above-outlined standpoint on the problem of combating crimes of

a terrorist nature, certain additions are also required in Chapter 28 of the Criminal Code of the Russian Federation, “Crimes in the Field of Computer Information.” Specifically, Part 1 of Article 272 of the Criminal Code should be amended as follows: “Access to legally protected computer information—that is, information stored on machine, computer, or computer systems or networks—shall be considered unlawful if it results in the destruction, blocking, modification, or copying of information, disruption of the operation of computers or computer systems and networks, or even if it results in the disclosure of legally protected computer information. . . .” The existing text would continue from there.

Part 1 of Article 274 of the Criminal Code should be amended as follows: “Violation of the rules for operation of computers or computer systems or networks by persons having access to computers or computer systems or networks that result in (1) the destruction, blocking, or modification of legally protected information; (2) the blocking of access to computers or computer network resources; or (3) the disabling of computer security systems, if any such actions have caused significant damage. . . .” The existing text would continue from there.

Article 6 of the Federal Law “On Operational Search Activities” sets forth a list of operational search measures. In the interests of bringing it into accordance with fundamental principles for combating terrorism, an additional point should furthermore be inserted to allow agencies engaged in such activities to decode encrypted electronic information. This also requires the amendment of Part 6 of Article 8 of the above-mentioned law: “The conduct of operational tests, the decoding of encrypted electronic information . . .” and so on as in the current text.

The above-proposed changes will make it possible to bring the Federal Laws “On the Militia” and “On Operational Search Activities” and criminal and procedural legislation into accordance with the Federal Law “On Combating Terrorism.” In addition, they will ensure the possibility of effective actions on the part of internal affairs agencies in the near term.

In connection with the problem under discussion, it must be noted that along with the development of computer technologies, genetic engineering and nanotechnologies provided society with more questions than answers in the last quarter of the twentieth century.

For instance, research on artificial intelligence and associated control procedures is being conducted at the University of Reading (Great Britain). Robots are being created that are capable of learning, interacting with one another, and reprogramming themselves independently. The main goal of the designers comes down to linking the human brain with the “brain” of the computer.

At U.S. universities such as Harvard, the University of California, and Princeton, research is being done on deciphering the codes of the nervous system in the aim of creating acceptable interfaces with the human brain. Furthermore, with the patronage of Congress and the White House, work is under way to devel-

op biotechnical systems comparable in size to atoms and molecules that possess logic and the capability of self-reproduction. The development of such technologies could lead to the creation of previously unknown forms of artificial life, cultivated by man for the supposed benefit of mankind. However, along with the development of nanosystems aimed at previously discovered cancer cells in the human body or the delivery of medicinal preparations to an ailing organ, experiments are also being conducted to collect the simplest mechanisms from molecules. These mechanisms, guided by internal signals, must manipulate other molecules and create more complex mechanisms, even including biorobots.

In this regard, it is also appropriate to cite a statement by a top Pentagon official: “We are approaching a level of development where no one is a soldier, but everyone is a participant in military actions. The task now is not to destroy living forces, but rather to undermine the goals, views, and outlooks of the population—to destroy the society.”

It is not by chance that I have cited these words, inasmuch as there have been reports in the media recently to the effect that the AIDS virus was also artificially created. According to these reports, it was developed in closed U.S. military laboratories, and as a result of an unsanctioned leak the virus spread around the planet.

High-tech inventions facilitate accurate diagnoses and the regulation of the mental and physical status of individuals, yet they also make it possible to evoke psychophysiological distress as a result of news of the latest research lab leak. There are no guarantees today that these inventions will not end up in the hands of terrorists of various types. Here it should be noted that the consequences of such a leak could be comparable to the results that would ensue if terrorists were to get their hands on a weapon of mass destruction.

For instance, U.S. laboratories are developing nanomechanisms the size of bees or even ants that can carry out any programmed functions from eavesdropping to shutting down electrical lines in response to commands transmitted from satellites or submarines.

There is also another point that cannot help but cause concern. The development of high-level computer technologies is at times linked with the relative simplicity and accessibility of preparing the means for possible terrorist actions. For example, one American inventor came up with the idea of an anticomputer cannon—a device that could disable computers, vehicles, medical equipment, and any other electronic devices from some distance away. The entire invention consists of a parabolic reflector, a horn-shaped antenna, and two automobile ignition coils, and it costs less than one hundred dollars. The cannon creates in its antenna a 20-MW burst of chaotic radio noise that is sufficient to change the normal operation of microcircuits. The impulse does not ruin a computer, but rather “freezes it up.” The use of this device can produce chaos in electronic transactions systems, including in operation of integrated databases, a most valuable resource for internal affairs agencies.

It is completely possible to state that problems related to combating terrorism in the high-tech sphere are among the most complex and little studied issues today. It is also an indisputable fact that an effective struggle against manifestations of high-tech terrorism is possible only with the establishment of international coordination of the activities of law enforcement agencies. And if the first step in the right direction lies in gaining a clearer understanding of problems related to preventing the use of high-tech developments by terrorists, then the second step must lie in creating a mechanism that would make it possible to prevent the spread of terrorist acts of this nature.

In my opinion, at least two stages can be defined in the construction of such a mechanism. The first stage must be tied to the development of guiding legal principles providing for the prevention of high-tech terrorism. At this stage, the possibility of criminal punishment for the illegal development, distribution, and use of bio- and psycho-computer systems should also be stipulated in national legislation. Furthermore, concerning Russia, we could also discuss the insertion of the appropriate corrections in the law "On Combating Terrorism." In particular, the concept of "informational-electronic space" should be added to Article 3 of this law, which presents a list of objects included in the sphere for conducting counterterrorist operations. It would also be expedient to make the corresponding addition to Article 1 of the European Convention on the Suppression of Terrorism (1977).

The second stage of the above-mentioned mechanism is connected with developing a control and monitoring format that facilitates effective implementation of the first stage.

In particular, in carrying out this second stage, the Russian Ministry of Internal Affairs faces the problem of how it should efficiently focus its organizational development in the future. Even today, one must raise the question of creating within the Ministry of Internal Affairs structure a special control-analytical agency that would monitor the spread of bio- and psycho-information technologies in Russia and prevent cases of high-tech terrorism. This unit should focus special attention on participation in the development (in cooperation with foreign partners) of approaches to combating terrorist manifestations in the high-tech sphere. It should also be involved in the exchange of experience and information on ways of countering the most dangerous types of criminal activity.

The effectiveness of the work of the above-mentioned unit will be substantially greater if the appropriate interactions are established with such organizations as the Russian Foreign Intelligence Service (SVR) and the Federal Security Service (FSB).

A consideration of the problem of combating high-tech terrorism also presupposes recognition by the country's population of the consequences of the increased role of information technology in the life of society. The results of a survey conducted by the author of this paper in the city of Moscow speak to this fact. Specifically, the following results were obtained regarding a problem that is not directly linked with cases of high-tech terrorism but is to a certain degree

characteristic of the level of legal consciousness among citizens. For instance, among survey respondents who were employees of organizations involved in computer hardware sales, a majority had a negative attitude toward the activities of the Microsoft branch office in Russia aimed at protecting the company's interests in the computer software market. In particular, about 90 percent of the respondents believed that Microsoft's activities are of the unceremonious nature of a monopolist dictating his own rules of the game. However, for some reason, no attention is paid to the fact that when selling licensed software, both the company representatives and the local dealer companies pay significant sums of money to the state in the form of taxes. When pirated software products are distributed, the state not only loses such an opportunity, but also in essence promotes the legalization of illegal actions in the high-tech sphere of societal activities. It is a well-known fact that terrorist manifestations become characteristic of those individuals who have previously gotten a taste for impunity. In the course of the survey, it was also established that approximately 30 percent of firms and organizations in this field of business have no interest in receiving information of a regulatory, legal, operational, or analytical character from law enforcement agencies through the agency for distribution of legal and criminal information that was recently created under the auspices of the joint publishing house of the Russian Ministry of Internal Affairs. Meanwhile, more 70 percent of respondents expressed their readiness to ensure the security of their own businesses (against racketeering, extortion, corruption, et cetera) over a network resource (the Internet) by means of establishing contacts with law enforcement agencies. Such figures should spur internal affairs agencies to step up activities in this direction, which could be viewed as promising in the sphere of preventing terrorism under information-based high-tech conditions.

In this regard, within the scope of this bilateral Russian-American seminar it is also of some interest to focus attention on the assessment made by internal affairs agency personnel of the abstract situation regarding criminal phenomena linked with the rising role of information technologies in the life of society. In response to a question concerning resolution of a case demanding a high degree of professionalism and restraint and offering opportunities for showing initiative in gaps in legislation, a case that is also contradictory and affects the lives of individuals, 45 percent of respondents (internal affairs agency personnel) chose the following behavior: do everything according to justice, both *de jure* and *de facto*. Furthermore, they felt that actions taken must not be hasty and must not transgress legal bounds. Another 20 percent preferred a skillful combination of the spirit and letter of the law in this situation, along with a striving to improve the legislation. Between 5 and 10 percent of the respondents preferred a flexible combination of the letter and spirit of the law in this case, without regard to conditions for implementing principles of humanity, justice, legality, and openness and without considering the need for the case to move through all of the procedural formalities, not to mention the sense of the

unusualness of the factual content of legal relations. About the same percentage of respondents preferred to hide behind the law and observe it to the letter, being guided by considerations of their own personal benefit. Only 10 percent of the respondents expressed readiness to do anything to achieve a just outcome in the case, even to the point of exceeding the bounds of their authority and placing themselves in a difficult position.

In conclusion, it should be noted that it is very urgent and timely to analyze the problems of countering terrorism under high-tech conditions, with internal affairs agencies being among the key actors in this countering effort. Such an analysis will also promote overall improvement of the legislative base and will increase the effectiveness of the activities of the Russian Internal Affairs Ministry system as information technology becomes ever more important in society. This all takes on special significance as the international information space continues to expand. The problems that might arise as part of this process can at times take on the most unexpected forms. One example of this is the attempt to bring two Chelyabinsk hackers to punishment in the United States after the Federal Bureau of Investigation conducted an operation to lure them out of Russia. In the current situation, Russian and U.S. law enforcement agencies, as the main actors in countering terrorism, are called upon to improve the procedures and methods of their work under high-tech conditions. They must not allow events to develop along “Chelyabinsk” lines, a situation that has given rise to a number of questions of a legal and moral-ethical nature in relations between the United States and Russia.

Papers from
*Terrorism—Reducing Vulnerabilities and
Improving Responses:
U.S.-Russian Workshop Proceedings (2004)*

Analysis of the Threats and Consequences of Terrorist Acts in Urban Settings: Outline of a Protection System

*Vladimir Z. Dvorkin**

Russian Academy of Sciences Institute of the
World Economy and International Relations

This report presents selected results of the project “Terrorism in a Megapolis: An Assessment of Threats and Levels of Protection,” which was completed in late 2002 by the Center for Political Research in Russia in cooperation with the Expert Innovation Center for Civil Defense and Emergency Situations and the National Anticrime and Antiterrorist Foundation.

The modern industrial infrastructure of highly developed states, in particular in megacities, includes many thousands of radioactive, chemical, and biological facilities and therefore presents a real opportunity for terrorists to inflict catastrophic damage even without using their own weapons of mass destruction, although their desire to obtain such weapons is clear.

The tragic events in New York City and Washington, D.C., on September 11, 2001, represented the end point in the process of realizing the threats from mass-scale terrorist acts, many dozens of which were committed in the last decade of the last century throughout the world. However, it is impossible to disagree with Senator Richard Lugar, who emphasized that regardless of how monstrous the September 11 tragedy was, the death, destruction, and panic were minimal compared with what would have resulted if weapons of mass destruction had been used.

This tragedy and the obvious threats of variations on it have added powerful impetus to efforts to strengthen cooperation in the world community in all areas related to combating international terrorism, including the military operation in Afghanistan, exchanges of intelligence information, the blocking of illegal fi-

*Translated from the Russian by Kelly Robbins.

nancial channels, and the strengthening of control and protection measures for radioactive, chemical, and other materials.

Separate mention should be made of the sharply increased number of publications on problems regarding the analysis of sources, characteristics, and potential of international terrorism and ways of countering its threats. Several of these research areas are distinguished by their completely adequate scientific depth and logic; however, there is a clear lack of systemic research on the problems. At the same time, theoretical and applied systemic research on these problems would seem more than urgent for the development of practical antiterrorism approaches, inasmuch as systemic principles for the study of any types of threats primarily call for the most exhaustive possible structured knowledge of the enemy, including its goals and objectives; financial, material-technical, and professional potential; weapons; and many other characteristics. Potential terrorist targets must be categorized by their degree of accessibility and the level of damage their destruction would entail. These data represent the necessary foundation for organizing anti-terrorism efforts. Bringing such research to an adequate level of completion requires the involvement of specialized organizations and a significant number of highly qualified professionals with experience working in these areas.

The results presented in this report are possibly the first (if not the zero) semblance of systemic research in this field. It does not claim to be a comprehensive presentation of all the issues listed above and is oriented primarily toward the problem of megacities.

An analysis of open informational materials and works on the problem of combating terrorist activities in megacities under the new conditions attests to the pressing need to develop a nearly exhaustive list of methods adequate to respond to the widest possible range of threats and types of terrorist activity. In addition to traditional methods, unique means without analogues in the military sphere may be used in the commission of terrorist acts. This is due to the fact that at its current stage of development, society is experiencing rapid and poorly controlled growth in the number of emerging ideas in the development and detailed study of fundamentally new strike effects. These ideas could serve as the basis for the accelerated creation of a wide and diverse array of technical means based on the application of physical, chemical, and biological principles and new technologies that were traditionally used by the terrorists of the past. A terrorist act could be planned over the course of years. The means to be used, the methods for using them, and the scope of the entire operation could be limited only by the availability of financial resources (often enormous) and personnel.

In addition, a certain backwardness of thinking has been observed toward the problem of counterterrorist activities in the political, operational-investigational, informational-analytical, and organizational spheres, and this backwardness gives rise to a shortage of fundamental support for timely decision making in the development of methods and means for conducting counterterrorist activities in megacities. One result of this could be difficulties in efficiently reorient-

ing existing forces and resources and focusing them to meet newly emerging threats. We see the appearance of a specific sort of loss of control over the process of developing means and methods for counterterrorist activities in the interests of ensuring security. Therefore, an orderly structure of recommendations on the ways and means by which terrorist activities are conducted must be developed, as well as decisions on how to combat them within that structure.

An analysis of the consequences and measures involved in fighting nuclear, chemical, and biological terrorism has long been under way, and some impressive results have been achieved. Significant attention is also being focused on how to counter computer and electromagnetic terrorism.

The latter topic merits additional explanation. The possibility of using powerful electromagnetic impulses as a means of attack has become absolutely real because of the development of sources capable of creating peak output on the order of several gigawatts and the miniaturization of the elemental components of military and civilian radioelectronics, which makes these devices vulnerable to extremely low levels of electromagnetic wave energy. Danger lies in the use of electromagnetic signals against the components of computers, which are widely used in systems for managing vital public services in megacities, controlling technological processes in dangerous production facilities, and so forth.

Experiments have shown that components of distributed types of microprocessors and computers have crashed or stalled at field voltages in the ultrashort range on the order of 1 V/cm. At the same time, more complex systems (such as the PC-XT/AT and other more complex computers) were found to have problems with memory and display operations at the level of $E < 0.02$ V/cm. Unshielded general-use computers were most vulnerable to electromagnetic energy in the frequency range of 1–10 GHz.

A real device capable of producing a super-broadband electromagnetic impulse was developed in the late 1990s using military ammunition containing a common explosive substance. Such ammunition could in principle create an electromagnetic impulse of 0.1–1 MHz in length with an energy value of 0.1–1 kJ and a frequency band of several gigahertz. Progress in creating similar devices for stationary installation and multiple use was demonstrated for the first time in the United States in 1992 as part of the Mark N project.

Mobile generators mounted on heavy-duty trucks and having their own power sources have also been developed. The use of such generators would make it possible to bring down an unshielded system for public utility management in a megacity or a banking system, or it could disable control systems at dangerous production facilities. Therefore, these generators could be viewed as effective tools for carrying out terrorist activities.

The example of opportunities for electromagnetic terrorism attests to the expanding spectrum of violent means and methods of attack. This spectrum could also include space terrorism, which seems to be a far-off prospect. However, the growing number of orbiting satellites and the fact that third world coun-

tries will soon create their own space devices mean that the day is coming when space terrorism will be as realistic a possibility as the hijacking of an airplane. The commission of space terrorism would involve, first, the destruction of satellites and other space-based devices or the creation of obstacles that would hinder their normal operation. Second, it could involve the seizure and use of space-based devices to facilitate communications among terrorists or their use for terrorist military operations. Carrying out space terrorism is a task requiring significant financial, intellectual, and material resources; however, it would be inappropriate to fail to consider it as part of the arsenal of methods that terrorists might use in the future.

The listed means of terrorist acts are directly or indirectly related in varying degrees to their impacts on elements of megacities. These elements may be conditionally divided into the following three categories:

1. Elements of megacities that represent direct targets for attack. These include high-rise apartment buildings, places where large numbers of people gather, major transportation hubs, and so forth.

2. Elements through which terrorists plan to achieve their goals. This category includes water systems, through which contaminated drinking water could be widely distributed in one or more locations; various means of transportation; the postal system (mass or targeted delivery of potentially dangerous mail or freight); various computer networks; and so forth.

3. Elements of megacities that represent sources of heightened danger, the destruction or disruption of which would cause wide-scale accidents and catastrophes entailing consequences comparable to those resulting from the use of weapons of mass destruction. Objects in this third category primarily include facilities located in or near the megacity, such as various enterprises in the atomic and chemical industries, research centers that operate nuclear reactors or use dangerous radioactive materials, petroleum storage facilities, and so forth.

It should be noted that terrorist acts directed at sites in the third category and using methods aimed at artificially causing wide-scale accidents could have the most dangerous consequences and therefore require more detailed study consideration.

Despite the measures being taken to make industrial production facilities, the energy industry, and means of transportation more secure and environmentally safe, tendencies toward increasing the scope and level of danger of accidents have been observed. This is the result of the introduction and rapid implementation of new technologies; the inclusion of new substances with toxic, flammable, aggressive, and other harmful properties in production processes; increases in the energy requirements of production; increases in the power of individual pieces of equipment, the size of storage facilities, and the capacities of cargo vehicles; and increases in the speed of production and distribution processes.

The potentially destructive forces inherent in production facilities and technologies create the objective foundation for their focused use as means of attacks aimed at inflicting damage on the regions in which they are located. This could be accomplished by artificially creating conditions necessary for releasing and taking advantage of their destructive potential. Some examples include

- the creation of zones of catastrophic flooding by destroying dams
- the radioactive contamination of an area by destroying nuclear reactors
- the chemical contamination of the atmosphere and water by destroying chemical plants
- the setting of massive fires by burning forests or oil and gas wells
- the spreading of epidemics

It is clear that a megacity's industrial facilities and high population density make it very vulnerable to dangerous forces of an industrial nature that would be unleashed upon the destruction of such facilities by terrorist groups. In this case, nonnuclear means could be used to trigger other factors with uncontrolled and wide-scale destructive effects. As a result, industrial facilities and technologies could be viewed as weapons of mass destruction (WMD), with an attack on them representing a passive form of WMD warfare.

In compiling a list of potentially dangerous facilities in a megacity, we used the results of an analysis of the potential consequences of their destruction.¹ An example of such a list is presented in Table 1. This list, however, does not allow for the ranking of the facilities found in megacities by the level of threat they face from terrorists. This could be done using the following characteristics:

Accessibility of facilities to terrorist attacks:

1. no limitations on access—no services for maintaining overall order at facility
2. no limitations on access—facility has services for maintaining overall order
3. limited access to facility
4. facility under armed guard

Technical means required for carrying out terrorist attack:

1. common military weapons or up to 1 kg of explosives
2. more than 1 kg of explosives
3. vehicles, heavy weapons, or a substantial quantity of explosives
4. dangerous radioactive, chemical, or biological substances
5. special equipment or unique weapons not in the arsenals of troops of the ministries of internal affairs or defense

TABLE 1 Example of a List of Potentially Dangerous Facilities

Type of Industry	Facility or Type of Production (Technology)	Basic Types of Damage Factors	Possible Impact Exclusion Zones, km ²
Electric Power	Located inside city limits or proximal to megacity:		
	• nuclear reactors at atomic power plants	Explosions, fires, radioactive contamination	Up to several hundred km ²
	• storage facilities for spent nuclear fuel	Explosions, fires, radioactive contamination	From tens to several hundred km ²
	• dams at hydroelectric plant reservoirs	Flood surge	From tens to several hundred km ²
Atomic Power	Processing of spent nuclear fuel:		
	• radiochemical plants	Explosions, radioactive contamination	Up to several thousand km ²
	• spent fuel storage facilities		
Fuel	Extraction and processing of oil and gas:		
	• oil and gas refineries, including units producing ammonia and other powerful poisons	Explosions, massive fires, chemical pollution of atmosphere	From tens to several hundred km ²
Pulp and Paper	Bisulfate production of pulp using powerful poisonous substances	Explosions, massive fires, chemical pollution of atmosphere	From tens to several hundred km ²
Food	Refrigerated processing and storage facilities	Explosions, massive fires, chemical pollution of atmosphere	Up to several km ²
Public Utilities	Water treatment plants and purification facilities	Explosions, massive fires, chemical pollution of atmosphere	Up to several km ²
Agriculture	Storage facilities for anhydrous ammonia and ammonia water for use as soil fertilizers and defoliators for cotton and other crops, central stockpiles of chemical pesticides and herbicides	Explosions, massive fires, chemical pollution of atmosphere	Up to several km ²

TABLE 1 (Continued)

Type of Industry	Facility or Type of Production (Technology)	Basic Types of Damage Factors	Possible Impact Exclusion Zones, km ²
Microbiological	Scientific research centers and test facilities: <ul style="list-style-type: none"> • production of biological agents and mixtures • production of biological livestock feed additives harmful to humans 	Pollution of atmosphere and local biospheres	Up to several km ²
Transportation	Railroad tank and freight cars, tanker trucks, marine tankers, and cargo freighters	Explosions, fires, radioactive or chemical contamination of the environment	Up to several km ²
Chemical	General chemistry: <ul style="list-style-type: none"> • production of powerful poisonous substances (chlorine, ammonia, phosgene, hydrocyanic acid, organophosphorus compounds, anhydrous sulfur dioxide, hydrogen fluoride, inorganic acids, etc. • nitrogen and phosphate fertilizers • chemical herbicides and pesticides • chemical fibers and threads • synthetic dyes, resins, and plastics 	Explosions, fires, chemical contamination of the atmosphere and water	From tens to several hundred km ²

Level of expertise required for carrying out terrorist attack:

1. skills in handling firearms or minimal knowledge of explosives
2. experience in working with explosives, expertise in evaluating the direction and destructive potential of explosions
3. knowledge of specific details regarding the operation of the target facility, high level of skill and expertise in handling specialized equipment or dangerous special substances

Frequency of occurrence of conditions under which terrorist act would cause maximum damage:

1. constant
2. daily during peak hours
3. several times per month
4. several times per year
5. unique conditions that might be repeated only once every few years

Consequences of terrorist act at facility:

1. several dozen victims, localized damage, insignificant economic damage (on megacity scale)
2. about 100 victims, several square kilometers suffering destruction or contamination, normal life of the city paralyzed for several days, substantial economic damage
3. several hundred victims, tens of square kilometers suffering destruction or contamination, city infrastructure disrupted and requiring several weeks or federal government funds and resources to restore, economic damage comparable to the annual city budget
4. several thousand victims, several hundred square kilometers suffering destruction or contamination, consequences beyond the megacity, event of nationwide scope

A categorized list of a megacity's critical (most vulnerable) potential terrorist targets, including transportation networks, places where large numbers of people congregate (stadiums, shopping malls), chemical enterprises, research reactors, water supply sources, electric power plants, and so forth, ranked in terms of the above-listed criteria, would include more than 50 groups of facilities.¹ Rankings of points in megacities vulnerable to terrorist attack are captured in Table 2.

This list is one of the fundamental components in the development and implementation of the comprehensive targeted program "Megacity—Capital" (TsKP MS). The goals of the program are to create, introduce, and develop an integrated system for combating terrorism. Its objectives are to coordinate the efforts of the various ministries, departments, organizations, and institutions regardless of level of jurisdiction or form of property ownership with the aim of achieving the stated goals.

The Megacity—Capital Program must be an integrated set of subprograms linked through resources, implementers, and timetables. The subprograms include taking inventory, systematizing, classifying, identifying, and evaluating the characteristics and vulnerability levels of all of the megacity's high-risk industrial facilities and natural sites both as potential terrorist targets and as

TABLE 2 Example of a Categorized List of Critical (Most Vulnerable in Terms of Terrorist Threat) Points in a Megacity

Name of Megacity Facility	Typical number of facilities in megacity	Accessibility of facility	Technical means required for attack	Level of expertise required for attack	Frequency of conditions needed for maximum damage	Consequences of terrorist attack
Atomic power industry facilities in or close to megacity:						
• nuclear power plant	1	4	2–4	3	1	2–4
• spent nuclear fuel storage facilities	1–2	4	2–4	3	1	2–4
Industrial facilities:						
• chemical plants and enterprises using radioactive materials	about 40	4	2 or 3	3	1	2–4
• oil and gas refineries, including units producing ammonia and other powerful poisons	2–3	4	1–3	1 or 2	1	2–4
• petroleum depots	2–4	4	1 or 2	1 or 2	1	1–3
• water treatment stations with stockpiles of 330–350 tons of chlorine at each	4–6	3	1 or 2	1 or 2	1	1–3
• ammonia storage facilities at refrigeration plants (10–120 tons) or wholesale produce enterprises (2–170 tons)	about 10	3	1 or 2	1 or 2	1	1–3
• liquid rocket fuel plants (hydrazine, asymmetric dimethylhydrazine, dinitrogen tetroxide, etc.)	1–2	4	1 or 2	3	1	1–3
• explosives plants	3–6	3	1 or 2	1–3	1	1–3
• pulping plants using bisulfates and other powerful poisonous substances	2–4	3	1 or 2	1–3	1	2 or 3

continued

TABLE 2 (Continued)

Name of Megacity Facility	Typical number of facilities in megacity	Accessibility of facility	Technical means required for attack	Level of expertise required for attack	Frequency of conditions needed for maximum damage	Consequences of terrorist attack
• coking plants and facilities producing anhydrous sulfur dioxide, sulfuric acid, and other powerful poisonous substances	1–2	3	1 or 2	1–3	1	2 or 3
• storage facilities for anhydrous ammonia and ammonia water for use as soil and fertilizer and defoliator for cotton and other crops, central stockpiles of chemical pesticides and herbicides	3–5	3	1 or 2	1–3	1	2 or 3
• plants producing biological agents, mixtures, and livestock feed additives harmful to humans	2–4	3	1 or 2	1–3	1	1–3
• synthetic rubber factories	1–3	3	1–3	1–3	1	1–3
• chemical plants using synthetic organics (phenol, aniline, benzene)	about 10	3	1–3	1–3	1	1–3
Megacity water supply system:						
• water mains and wells supplying the city with drinking water	about 10,000 km	2	1 or 4	1 or 3	1	1 or 2
• water treatment facilities	20–30	3	1 or 4	1 or 3	1	1 or 2
• boiler plants	about 100	3	1 or 2	1	1	1
• sewer system	5000–6000 km	1	1 or 2	1	1	1
• storm drain network	about 6000 km	1	1 or 2	1	1	1
• water intake points	10–15	3	1 or 4	1 or 3	1	1 or 2

TABLE 2 (Continued)

Name of Megacity Facility	Typical number of facilities in megacity	Accessibility of facility	Technical means required for attack	Level of expertise required for attack	Frequency of conditions needed for maximum damage	Consequences of terrorist attack
City energy supply system:						
• gas pipelines and propane tank filling stations	about 100	2	1	1	1	1 or 2
• power plants supplying the city with electricity	20–25	4	2 or 4	1 or 2	1	1–3
• electric power lines	several thousand km	1	1	1	1	1
• substations	about 150	1	1	1	1	1
Places where large numbers of people gather:						
• stadiums	about 50	2	1–3	1–3	3	1 or 2
• movie theaters and concert halls	about 90					

possible sources of industrial accidents, catastrophes, and natural disasters. Other subprograms involve the development of a unified conceptual and terminological framework and a set of laws, regulations, and reference documents, as well as the implementation of a series of special research, design, industrial, socio-economic, organizational, and other measures to ensure the effective handling of security problems related to combating high-tech terrorism. Integrating all existing security and public service systems will make it possible to create a systematic basis for protecting the population, facilities, and territories from various types of external and internal threats.

The difficulty in developing and implementing the comprehensive program for countering terrorism in megacities can, on the one hand, be overcome by organizing the system into threat classes, for example, radiation, chemical, radiological. However, in doing so, it would be even more difficult to categorize and identify the top priority targets for protection given the limits on available

resources. On the other hand, it would be expedient to develop and test procedures for implementing such a program in a typical district of a megacity, one that includes examples of the types of facilities that would be potential terrorist targets.

More detailed materials on the problems mentioned above may be found in the previously cited publication of the Center for Political Research in Russia, which its authors believe to be the first systematic attempt at a comprehensive analysis of the problems of combating terrorism in megacities. The publication also provides a basis for the initiation of a more in-depth systematic analysis of these problems and the development of a set of practical recommendations and organizational and technical measures for effectively meeting these new security challenges.

NOTE

1. Terrorism in a megapolis: assessment of threats and levels of protection. 2002. Moscow: Human Rights Publishers.

Lessons Learned from the *Nord-Ost* Terrorist Attack in Moscow from the Standpoint of Russian Security and Law Enforcement Agencies

*Yevgeny A. Kolesnikov**
Russian Federal Security Service

It was not today or even yesterday when terrorism arose as a social phenomenon. Political terrorism became an international problem at the start of the twentieth century. While the activities of extremists were previously of a targeted nature, in our times they have victimized not only state leaders and prominent public and religious figures but also completely random citizens, and in most cases the terror strikes have been directed against these very individuals.

The tragic events that occurred in Moscow on October 23, 2002, represent one link in the chain of acts committed by international terrorists. At 9:05 p.m. that day, an armed band of terrorists headed by the Chechen field commander Movsar Baraev seized the Palace of Culture of the Moscow Ball-Bearing Factory, where a performance of the musical *Nord-Ost* was under way. There were more than 900 people in the building, including theater personnel.¹

This act may be placed in the same category as crimes committed by members of al Qaeda, the Taliban, and other international terrorist organizations in the United States, Indonesia, and various countries of the Middle East. There is no doubt that this act represents the latest manifestation of international terrorism in its most extreme form and should be viewed as a blow against the entire international security system, affecting the interests of all civilized states. The true goal of the act was to harm the territorial integrity and security of the Russian Federation.

At 9:30 p.m. on October 23, 2002, dispatch services of the Federal Security Service (FSB) and internal affairs agencies received reports that a group of terrorists had seized a large number of hostages at the Moscow Cultural Center of

*Translated from the Russian by Kelly Robbins.

the State Ball-Bearing Factory, located at 7 Melnikov Street. At 9:35 p.m., after the reports were checked and verified, an alarm went out to special services personnel. Information on the seizure of the hostages was relayed to the president of the Russian Federation, the heads of federal ministries and agencies, and the Moscow city authorities.

In order to handle the situation and coordinate efforts to free the hostages, an operational headquarters was established, including representatives of the FSB, the Ministry of Internal Affairs (MVD), the Ministry of Emergency Situations, the Ministry of Defense, city administrative and management agencies, the Committee on Health Protection, and other specialists in rendering urgent aid in extreme situations.

On orders from the operational headquarters, heightened security was put in place around official government buildings and critically important elements of the city's infrastructure. Law enforcement units, special operational response detachments, personnel from the Ministry of Emergency Situations, and emergency medical and fire brigades were deployed in the area of the tragedy. The area was surrounded by police forces and MVD troops.

In accordance with plans that had been developed, forces from specialized detachments in the area deployed a mobile command center. A round-the-clock communications channel was established to exchange information with representatives of law enforcement agencies and special services of foreign states accredited in Moscow, which had provided detailed information on their countries' citizens who were among the hostages as well as offers of practical and technical assistance. Regularly scheduled briefings were organized for these partners.

Working under severe time constraints, the operational headquarters had to take many varied aspects of the situation into account. Thus, as new information was coming in about the circumstances surrounding the hostage taking and the situation inside the building, efforts were simultaneously under way to prepare action plans for various scenarios under which events could develop.

Already on October 23, the operational headquarters was informed of the existence of a facility identical to the Cultural Center of the Ball-Bearing Plant (the Meridian movie theater), and special assault units of the FSB Special Operations Center (SOC) began training exercises there. As a result of these exercises, on October 25, commanders of the operations units of the SOC outlined an overall concept for the military/law enforcement component of a possible special operation, developed various options for storming the building, and coordinated the details of cooperation with the various groups involved. They then informed the operational headquarters that they were standing ready to conduct the operation.

Meanwhile, the operational headquarters was also taking measures aimed at freeing the hostages by other means. International experience in conducting such operations has shown that although storming a building is, as a rule, extremely

effective, it very often entails threats to the hostages' lives. Therefore, storming the building was not seen as the only option for resolving the situation. The preferred method, which could produce positive results under certain conditions, was to remove the terrorists from the building through negotiations. The plan was to gradually improve the situation for the hostages and then either force the terrorists to completely or partially give up their demands or neutralize them so that they presented the least possible risk to the captive citizens.

With that in mind, the negotiation process was initiated with the terrorists by means of the hostages' mobile telephones. The terrorists' demands were learned, and an understanding was reached regarding the parties with whom the terrorists were prepared to negotiate. Telephone contacts maintained with the hostages also made it possible to obtain information about what was happening in the concert hall on a real-time basis. To develop a scenario of what had occurred, individuals who had witnessed the seizure of the building were questioned on orders from the operational headquarters. Members of the Duma and representatives of public organizations and the media were included in the process of negotiations with the terrorists.² As a result of the negotiations, several groups of hostages were freed, including children less than 10 years of age.

From the first hours of the tragedy, the special services units involved took measures to assist the hostages. For instance, at 11:40 p.m. on October 23, during a reconnaissance of the perimeter of the theater complex, a metal door was discovered leading to a nightclub in the complex. Cries for help could be heard coming from inside. Following appropriate safety precautions, the door was opened, and about 40 people were freed from the building. During a search of basements, roofs, and the interior courtyard of the complex, three more escaped hostages were found. An SOC officer was wounded in a shoot-out with the terrorists while covering two women who had jumped from the second story of the Cultural Center. Overall, 113 people were freed by various means before the building was stormed.³

Officers from the screening group questioned the freed hostages and the individuals who had served as intermediaries in the negotiations. In particular, it was established that the terrorists were actively using methods of psychological pressure on the hostages and their relatives outside the building that had been seized. By telephone the terrorists were demanding that the relatives organize and conduct protest demonstrations in Moscow calling for the removal of federal troops from the Chechen Republic and the granting of independence to Chechnya. Out of fear for their loved ones, the relatives of the hostages were forced to attend those demonstrations.

Furthermore, to ensure their control over the situation in the concert hall, the terrorists used well-known psychological tactics by which some hostages characteristically begin to experience feelings of gratitude towards their captors under periods of stress despite the harsh treatment they are receiving. Thus, the hostages were for a long time deprived of food, water, and the ability to move

around in the hall and were subjected to humiliations in performing essential natural functions. According to the estimations of health care specialists, hypodynamia, exhaustion, and dehydration had set in, with these conditions being capable of producing lethal consequences. The goal of these inhuman actions on the part of the terrorists was to subjugate the will of the hostages.

Based on information coming in from various sources, a map was drawn showing the placement of the terrorists and hostages and the locations where explosive devices had been set. From an analysis of the information received during the range of search, tactical, organizational, and technical operations that were carried out, the following scenario emerged. About 1,000 hostages were being held by a group of 35–40 terrorists in the auditorium of the Cultural Center. Two powerful explosive devices had been placed in the center of the hall and on the balcony, and mines had been placed on the stage and aimed into the auditorium. Some 15–18 female suicide bombers wearing belts with explosive devices were deployed around the perimeters and in the center of the seating area.

Terrorists armed with automatic weapons and grenades were located on the stage and in the balconies. Powerful explosive devices had possibly been placed under the weight-bearing structural supports of the building. The bandits had established observation posts and fire points in technical and maintenance areas on the second and third floors, making it impossible for tactical groups to make a covert entry into the Cultural Center building. In the opinion of explosives specialists, the simultaneous detonation of the explosive devices would have led to the complete destruction of the building and the certain deaths of all the hostages and tactical team members (more than 1,000 people).

It should also be noted that the number of victims could have been twice as high. There were 17 buildings in the restricted zone around the Palace of Culture alone. Of them, 10 were directly facing the building that had been prepared for detonation. The average distance from these buildings to the Palace of Culture was approximately 200 m. The structures included a military hospital, an educational institution, factory facilities, and apartment buildings, all of them hooked up to natural gas pipelines. If an intentionally or accidentally initiated explosion were to occur, the blast wave or debris could damage the gas lines. If sparks or pieces of burning debris were to fall into the factory grounds, they could ignite tanks of fuel or other chemical reagents or set off explosions of oxygen tanks—in other words, a major industrial catastrophe could result.

The operational headquarters took measures to resolve the situation peacefully, but it was not possible to achieve the desired results. The position taken by the terrorists ruled out any possibility of seeking a compromise solution. It was established that Baraev was not an independent figure and that decisions were being made by individuals located not only outside the building but also outside the borders of Russia. The terrorists' reconsideration of the agreement to release the foreigners, Baraev's October 25 statement that they would begin shooting

the hostages at 6:00 a.m. on October 26, the deaths of four people (one woman and three men who were shot), and the previous behavior and personal characteristics of the terrorists reduced the chance of a peaceful outcome of the negotiations to zero and served as the basis for the decision to storm the building.⁴

From 5:00 to 5:30 a.m. on October 26, after all the necessary security measures were taken, assault teams were moved into their initial positions. It was obvious that in order to neutralize a large group of well-prepared terrorists with established positions in a building with a large number of rooms, individuals who had not only firearms but also an enormous array of explosives deployed in direct proximity to the hostages and at the most vulnerable points in the building's structure, the situation required an extraordinary plan of action that would preclude the possibility of any explosion. Therefore, the forward deployment of the assault teams was preceded by the use of special gas, which according to the plans of the operation's leadership would sharply reduce the capacity of the terrorists for resisting the assault. Taking into account the fact that the gas could affect the hostages as well, additional emergency medical service personnel supplied with the necessary antidotes were moved in close to the building.

As for the characteristics of the gas and the concentration used, these were selected by specialists with experience in this area. Fentanyl-based gas is widely used in surgery throughout the world, and it facilitates the temporary reduction of patients' movements without threatening their lives or health.

The assault teams included explosives specialists. The teams gained entry to the building through three access points—the nightclub, the central entrance, and the lobby windows. In a very short time, after overcoming the armed resistance of the terrorists, the assault teams burst into the auditorium and began defusing the explosive devices and evacuating the people.

During the special operation, which resulted in the elimination of 41 fighters led by Movsar Baraev, more than 750 hostages were freed, including 60 foreigners. Four members of the special forces units were wounded; two of the four were hospitalized. A number of individuals suspected of being accomplices to the terrorists were also detained during the course of the special operation around the theater complex.

Emergency medical assistance was provided to all the victims; however, 129 people died, including 8 foreign citizens. With regard to these victims, the loss of whom was unfortunately impossible to avoid, the main factors that increased the likelihood of their deaths were as predicted by health care specialists, namely stress, hypodynamia, hunger, dehydration, and the consequent exacerbation of preexisting illnesses, which are absolutely to be expected in people in a weakened state.⁵

During the operation, many automatic weapons, ammunition, and 76.6 kg of explosives were discovered and taken from the terrorists, including 17 automatic rifles, 20 handguns, 25 homemade explosive devices, so-called suicide belts, 2 homemade bombs in the form of metallic tanks filled with OF-540 artillery

shells (with a total weight of 12 kg of explosives), 106 grenades (90 of which were homemade from VOG-17M and VOG-25 grenades for automatic grenade launchers), and more than 5,000 rounds of ammunition.

These are the basic figures characterizing the results of the operation. However, an analysis of the events of those days provides a basis for a broader range of conclusions and evaluations that have been drawn not only by law enforcement agencies and the special services but also by Russian society in general. Even the most reliable arguments pointing out that casualties were unavoidable under the circumstances and that there would have been far more victims if the start of the special operation had been postponed will not bring back those whose lives were taken by the plague of our times, international terrorism.

The Moscow city prosecutor's office has initiated criminal case No. 229133 based on Article 30 Part 3 (preparation for crime), Article 205 Part 3 (terrorism), and Article 206 Part 3 (hostage taking) of the Criminal Code of the Russian Federation.

Evidence gathered during the investigation includes documentation of repeated attempts to force Russia's senior leadership to hold talks with Aslan Maskhadov, as well as the prerecorded message from the terrorists that was broadcast by the al-Jazeera network, the psychological pressure that was placed on the hostages to force them to sign an appeal to the Russian president, the placing of telephone calls to the hostages' relatives and to the media asking them to organize and conduct rallies in support of the terrorists' demands, and the well-developed campaign conducted in the media. All of this evidence illustrates once again that the action was planned in advance and was supported in circles opposed to Russian government policy in the North Caucasus.

By means of coordinated investigations and operational efforts, the Moscow city prosecutor's office, the FSB, the Main Administration for Combating Organized Crime of the MVD Criminal Militia Service, and the Moscow Main Administration for Internal Affairs have done a great deal of work to clarify the circumstances of the hostage taking, determine who actually participated in the terrorist act, uncover the connections between the terrorists and their accomplices, and obtain information about terrorist acts that might be in preparation.

An analysis of the evidence gathered during the investigation illustrates the unbreakable link between this crime and the designs of the ideologists of international terrorism, who plan and finance broad-scale terrorist acts throughout the world. The methods used in developing and implementing the preparatory phase and the act of hostage taking itself were characteristic of those used by extremist organizations associated with al Qaeda, the Taliban, and other criminal groups espousing terrorism and violence as a means of achieving their goals.

The unshakable links between international terrorist organizations and fighters operating in the North Caucasus are also confirmed by the fact that Baraev's bandit group included foreign citizens from the Middle East. International terrorist leaders were involved in preparing and committing the terrorist act. They

provided moral and material support to Baraev's group, including support sent from abroad, and took part in the leadership of this act. This is illustrated by the repeated attempts made immediately before the terrorist act, including some attempts from abroad, to force Russia's senior leadership to negotiate with Aslan Maskhadov.

Among the materials gathered for the criminal case are a video cassette of an interview given by Maskhadov on October 18, 2002 (five days before the events), in which he threatens to carry out terrorist acts, and a video of an August 2002 meeting of Maskhadov, Shamil Basaev, Movsar Baraev, and Abu Omar, the Arab mercenary and spiritual mentor of the fighters, at a conference of bandit group leaders in the Chechen Republic, where Baraev received his final orders and blessing to carry out the planned act.

In addition, evidence has been gathered indicating that not only Maskhadov and Basaev but also such major international terrorist figures as Movladi Udugov and Zelimkhan Yandarbiev were involved in planning and carrying out this crime. It should be noted that the latter two criminals are living abroad fully legally and are continuing their vigorous anti-Russian activities.

Up to now, the bodies of 34 of the fighters who were killed have been identified, and efforts are under way to identify the other 7.⁶ Investigations are being conducted to determine the routes by which the terrorists traveled and the channels through which they obtained weapons and explosives. The routes and means of transportation (rail, air, or bus) used by some of the fighters have already been established. Official inquiries have ascertained that some of the terrorists were using passports with false information. One channel has been discovered through which false documents were created and delivered to the fighters. Operations and investigations are still under way in connection with three individuals in custody. Individuals involved in recruiting the female suicide bombers have been identified and are being sought.

Information has been received indicating a connection between the car bombing at the McDonald's restaurant on October 10, 2002 (2 Pokryshkin Street, Moscow) and the seizure of the hostages at the Palace of Culture of the Moscow State Ball-Bearing Factory. Expert assessments have established that the types of homemade explosive devices used in both incidents were identical. Certain individuals have been discovered to be involved in both cases.

During their operations, investigators have uncovered apartments used by the terrorists who participated in the hostage-taking incident. These apartments were also used as transfer points for the storage of weapons and explosives. When these locations were searched, officers found and seized firearms, ammunition, communications devices, and other equipment for carrying out terrorist acts, including 21 belts used in making *shahid* belts for the female suicide bombers.

Of course, more information will become available after the investigation is completed. However, I would like to emphasize that the operation to free the

hostages on October 26, 2002, was and remains one of the most important landmarks in the struggle being waged by the law enforcement agencies and special services of the Russian Federation against the forces of terrorism. The events associated with the seizure of hostages at the Dubrovka theater complex revealed shortcomings in the organization of antiterrorism activities at the federal level, particularly with the process of providing information about the counterterrorist operation through the media. It is essential to understand clearly that the primary goal of terrorist acts is to attract broad public attention to certain processes, to instigate social confrontation within society, and to attempt to put pressure on the authorities and state administrative structures.

While noting the generally well-coordinated and selfless work done to free the hostages, we must also state that there are a number of problems objectively hindering the conduct of such operations. Many of them are of a narrowly specialized nature, and solutions for them are being worked out by the relevant agencies.

Cooperation between law enforcement and the media plays a special role in the process of resolving difficult conflict situations. During this operation, the operational headquarters could not achieve the necessary level of mutual understanding and coordination of actions with representatives of the media. Some correspondents covered the events associated with the freeing of the hostages in a tendentious manner and used the situation for their own particular aims. We must continue to work with journalists in improving our relationship in such situations.

The main conclusion to be made is that the overwhelming majority of citizens supported the action that was carried out, which attests to the consolidation of all segments of society in opposing attempts to destroy the Russian Federation and supporting the struggle against extremism and its ultimate form, terrorism.

We are deeply grateful to the international community for the support provided to Russia in those tragic days. Special thanks go to law enforcement agencies and special services of the partner states that declared their readiness to participate directly in efforts to free the hostages and in the investigation of the circumstances surrounding this crime.

Russia is ready to do everything in its power to promote measures to disseminate the experience it has gained in conducting such special hostage rescue operations, to exchange information on the weapons and equipment used, and to organize joint training exercises for both command and special operations units.

NOTES

1. At least 920 people were taken hostage, including 111 minors (39 of whom were small children), a number of pregnant women, and 68 foreign citizens.

2. Those involved in the negotiations included Iosif Kobzon (October 24, 1:37 p.m. and 3:35 p.m.), Irina Khakamada (October 24, 3:35 p.m.), Leonid Roshal (October 24, 5:50 p.m.; October 25, 1:37 a.m. and 2:50 p.m.), Grigory Yavlinsky (October 24, 11:37 p.m.–12:58 a.m. October 25), Anna

Politkovskaya (October 25, 2:50 p.m. and 7:40 p.m.), Sergei Govorukhin (October 25, 5:00 p.m.), Dmitry Beletsky (October 25, 5:00 p.m.), Yevgeny Primakov (October 25, 7:40 p.m.), Aslanbek Aslakhanov (October 25, 7:40–8:24 p.m.), Ruslan Aushev (October 25, 7:40 p.m.), *Sunday Times* journalist Mark Franchetti (October 25, 3:15 p.m.), four journalists from the Russian television network NTV (October 25, 1:40 a.m.), two Jordanian doctors (October 24, 5:50 p.m.), and five representatives of the Red Cross (October 25, 12:00 noon).

3. Of the 113 people freed before the building was stormed, 69 escaped (including 5 children) and 44 were rescued (including 25 children under age 14 and 3 older teenagers).

4. The following people were shot by the terrorists: (1) Olga Nikolaevna Romanova, born 1976, salesperson at the L'Etoile store in Moscow; (2) Konstantin Ivanovich Vasiliev, born 1967, chief specialist in the personnel department of the Main Administration for Military Court Operations of the Supreme Court of the Russian Federation; (3) Denis Petrovich Gribkov, born 1972, glassblower from the Laser-Neon company in Moscow; and (4) Pavel Georgievich Zakharov, born 1979, engineer from the Federal Registry of National Building Codes and Standards in Moscow.

5. According to data from the Moscow City Healthcare Committee, 650 people (including 9 children and 32 foreign citizens) were released from inpatient treatment facilities after rehabilitation.

6. Of the 41 terrorists killed, there were 19 women and 22 men. Thirty-four have been identified, and seven bodies (one woman and six men) remain to be identified.

Technical Protection of Electronic Documents in Computer Systems

Valery A. Konyavsky

Scientific Research Institute of Problems of Computer Technology and Information
Russian Ministry of Communications and Information

Information results from the reflection of the movement of material objects in living systems.¹ It circulates in company with similar organisms in the form of data and reports. Data are formed as a result of the reflection by these organisms of material objects, including reports. Reports are formed as organisms for the transmission of data to other organisms. They contain the totality of data being transmitted and represent a selection of signs with the help of which data may be transmitted to and received by another organism.

The transformation of data into reports and reports into data is carried out by individuals using algorithms for coding and decoding the set of symbols received into the elements comprising its “information” model of the world. Thus, information in the form of data is born in the minds of individuals (and only there) and cannot be protected through technical means.

Until recently, the problems of technical protection were reduced to the protection of computers from unauthorized access, the limitation of access to data, and network protection. Paradoxically, at none of these stages was there any discussion of what exactly we were protecting. It is obvious that if a plant produces teapots and a factory makes boots, then they will be potential targets for crime. Computer systems do not produce information. They process certain reports and elaborate others. But what does the information system produce? What should be protected? If we agree that it does not produce information, then it remains to be determined exactly what it does produce.

The results of information systems operations include spam (informational trash) and electronic documents. What is not deemed a document is just a useless scrap of paper. Structured and combined together, electronic documents repre-

sent information resources, which have value when—and only when—they are complete, authentic, accessible, and current.

For a report to be an electronic document, it must include a number of attributes attesting to its compliance with special requirements of high-tech end products deemed by society to have legal weight. It must adhere to technical and technological requirements for document creation and transmission, points that must also be documented by various generally recognized means.

Again, information systems produce electronic documents, a process that involves elements such as

- computers
- data (other electronic documents)
- network (telecommunications) resources
- information technologies

One important information security-related event that has occurred in the last decade is the appearance and development of the concept of device security. The main ideas of device security include the following:²

- recognition of the multiplicative protection paradigm and, as a result, equal attention to implementation of control procedures at all stages of information systems operations (the protection of the entire system is no greater than the protection of its weakest link)
 - “materialist” resolution of the fundamental question of information security: “What first—hardware or software?”
 - consistent rejection of software-oriented control methods as obviously unreliable (attempts to use software to monitor the correctness of other software is equivalent to attempting to resolve the unsolvable question of self-applicability—“Munchausen Syndrome”) and the shifting of the most critical control procedures to the device level (Archimedes’ principle), in accordance with which “support points” must be created to carry out device-based control procedures
 - maximum possible separation of condition-stable (software) and condition-variable (data) elements of control operations (divide-and-conquer principle)

The need to protect information technologies has only recently been recognized. Up to now, the public has defined an electronic document as a file signed with an electronic signature. This is incorrect. Here are two illustrations—a coded message and a piece of currency. Neither has a signature or a seal, but they are documents nonetheless. Why do we accept them as documents? Only because (and this is enough) we trust the technologies by which they were produced. If the commander of a military unit receives a coded message with orders from his command from the hands of the code officer, he has every reason to accept the text he has received as a document (order). And if he finds that same

text lying on his desk without knowing how it got there, then it is time to investigate the matter. Such investigations involve methods little known in broader circles. Matters are different with regard to the currency. Few of us ever receive bills directly from the printing plant. More often, the ways in which bills come into our possession are not completely known. Our behavior is also different—when we receive bills at a local branch of the state savings bank, as a rule we count them quickly, but if we receive them as change from a trader at the market, we might examine them more carefully for evidence they may be counterfeit.

Technologies for electronic exchanges must meet certified standards, and this compliance must be monitored. The various stages of the information exchange process involve people (operators, users) and information technologies—technical (personal computers, servers) and programmatic (operating systems, preprocessor output programs). Information is created by people, then transformed into data, and then entered into automated systems in the form of electronic documents, which together with other such documents represent information resources. Computers exchange data over communications channels. During the operation of automated systems, data (electronic documents) are transformed in accord with information technologies being applied. Therefore, we may identify the following seven components of technical security:

1. authentication of participants involved in information exchange
2. protection of hardware from unauthorized access
3. delineation of access to documents, personal computer resources, and networks
4. protection of electronic documents
5. protection of data in communications channels
6. protection of information technologies
7. delineation of access to datastreams

In working with the last component, protection is required not only for data in communications channels but also for the channels themselves. In fact, at present it is impossible to create a system of any large scale on these channels—it is expensive, ineffective, and unprofitable. It is almost impossible to make full use of a given channel. Existing channels are operating at barely 10 percent of capacity, which suggests the obvious conclusion, namely, the organization of virtual private networks using existing channels. This requires datastream tunneling; that is, data in various virtual private networks created over common channels must be isolated. Access to these data must be restricted.

Taken together in their entirety, points 1, 2, 3, and 5 and, in part, 7 also compose the focus of information protection as it is traditionally understood. It is obvious that this focus is actually much broader, including at least points 4 and 6. This fully explains the lack of significant successes in traditional approaches to resolving these problems in practice.

Having clarified this,² following are a few requirements for implementing the various levels of protection. As a house is built of bricks or other structural components, an information system is likewise built from various premanufactured elements, with only a small applied component being created from scratch, as a rule (although this newly created component is the most important, as it determines the functionality of the system). It is appropriate to recall the multiplicative protection paradigm, particularly that the level of information security of a system is no higher than that of its weakest link. For us this means that when using premade components we must select them so as to ensure that the protection level for each one is no lower than that required for the system as a whole. This applies to the protection of both information technologies and electronic documents. Lack of protection for either means that efforts in other areas are wasted.

AUTHENTICATION OF PARTICIPANTS IN INFORMATION EXCHANGE

Operator identification/authentication (IA) must be performed on a device basis at each stage in the operating system loading process. IA databases must be stored in the energy-independent memory of the information security system so that access to them via a personal computer would be impossible; that is, the energy-independent memory must be located outside the personal computer's address space. The control software must be stored in the controller's memory and protected against unauthorized modifications. The integrity of the control software must be ensured through the technology built into the information security system controller. Identification must be performed using an alienable information carrier.

As with operator IA, device-based procedures for remote user IA are necessary. Authentication may be handled through various means, including by electronic signature. A requirement for "intensified authentication" is becoming mandatory, that is, periodic repetition of the procedure during the work session at various time intervals short enough to prevent an ill-intentioned individual from doing significant damage if protection measures are thwarted.

PROTECTION OF HARDWARE FROM UNAUTHORIZED ACCESS

Means of protecting computers from unauthorized access may be divided into two categories: electronic locks and device modules for authorized loading. The main difference between them is the way in which integrity control is implemented. Electronic locks operate on a device basis to carry out user IA procedures, but they must resort to the use of external software to perform integrity control procedures. Device modules perform all the functions of electronic locks as well as integrity control and administration functions. As a result, these mod-

ules not only provide user IA but also handle the authorized loading of the operating system, a most important function in the construction of an isolated programming environment. Device modules handle a significantly wider range of functions than electronic locks, and they require device-based performance (not using operating system resources) of complex functions such as file system selection, reading of real data, and so forth. In addition, by integrating control functions into the hardware, device modules also offer greater reliability of results.

- **Control of technical integrity of personal computers and servers.**

Control of the integrity of personal computer components must be carried out by the information security system controller before the operating system is loaded. All resources that might be used must be monitored, including

- ♦ central processor
- ♦ system BIOS (Basic Input/Output System)
- ♦ supplemental BIOS
- ♦ interrupt vectors INT 13 and INT 40
- ♦ CMOS, including floppy disks, hard disks, and CD-ROMs

The integrity of the technical components of servers must be ensured through intensified network authorization procedures. These procedures must be carried out at the point at which the computer being verified logs on to the network and again at time intervals previously determined by the security administrator. Enhanced authentication must be implemented using the recommended type of random number generator device. The performance of the device must be monitored with a system of recommended tests.

- **Control of operating system integrity.** Control of the integrity of system components and files must be carried out by the controller before loading of the operating system, which is done through the mechanism of real data reading. Since the electronic document exchange process may involve the use of various operating systems, the controller's built-in software must handle the most popular file systems. The integrity of a given software package must be guaranteed by the technology of the data security system controllers. The controllers' devices must protect the software from unauthorized modifications. The well-known (published) hash function must be used to monitor integrity, and its standard value must be stored in the energy-independent memory of the controller protected on a device basis from access from the computer.

- **Control of applications software and data.** The integrity of applications software and data may be monitored by the data security system on a device or software basis if its integrity was registered on a device basis at the preceding stage. The well-known (published) hash function must be used to monitor integrity, and its standard value must be authenticated with the help of a remote technical data carrier (identifier).

LIMITATION OF ACCESS TO DOCUMENTS, COMPUTER RESOURCES, AND NETWORKS

Modern operating systems increasingly include built-in access limitation capabilities. As a rule, these capabilities utilize particular features of specific file systems and are based on attributes closely linked to one of the application program interface (API) levels of the operating system. This inevitably leads to problems, including at least the following:

- **Linkage to features of specific file systems.** As a rule, modern operating systems use not one but several file systems, both new and old. It usually happens that an operating system's built-in access limitations work with a new file system but might not with an old one, as they make use of substantially different features in the new file system. This circumstance is usually not directly addressed in the system documentation, which could lead the user to become confused. Let us imagine that a computer with a new operating system is running software developed for the previous version, which is oriented toward the features of an older file system. The user rightly assumes that the established security mechanisms, certified and intended for this operating system, will perform their functions, while in reality they will be turned off. In real life, such cases may be encountered fairly often. Why rewrite an application just because you have changed operating systems? Especially when the goal is to ensure the compatibility of old file systems and link them to new operating systems!

- **Linkage to the API of the operating system.** As a rule, operating systems now change frequently, once every year or year and a half. It is not impossible for them to change even more often. Some of these changes involve changes in the API, for example, the replacement of Win 9x with WinNT. Since the access limitation attributes are a reflection of the API, a move to an updated version of an operating system requires the reworking of security system additions, retraining of personnel, and so forth. Thus, we might posit the following general requirement: The subsystem for access limitation must be built on the operating system and be independent of the file system. Of course, the set of attributes must be sufficient for the purposes of describing the security policy, and the description must not be in operating system API terms but rather in terms that are customarily used by security administrators.

ELECTRONIC DOCUMENT SECURITY

The life cycle of the electronic document occurs in three spheres of existence, located concentrically one within the other: the electronic environment of numerical processes, the analogous environment of subjects and objects, and the social environment of cognitive subjects. The outermost layer is formed by the multitude of cognitive subjects of the social environment, which forms the sector

of activity for the document that dictates the rules of information exchange for its subject members, including requirements for interactive technology. If these rules and requirements are met, the report is deemed a document, while the information it contains is deemed by the sector as a (juridical) fact, a formal basis for initiating, changing, or terminating specific relations between subjects in the society.

The requirements of the sector of effectiveness may be divided into two categories: semantic, which are applicable to the representation of the meaning of the information, and technological, which dictate the formation of the document. The semantic aspects are the prerogative of the social environment and therefore are not considered in this paper and are deemed to be fulfilled. Given this condition, in order for a report to be recognized as a document, the parameters of the technologies used in its creation, transformation, transmission, and storage must fall within the bounds of allowable deviations from a certain standard prescribed by the sector for document-based electronic interaction. Only in this case do we have the legal grounds for considering that the requirements are met, for example, with regard to ensuring the integrity, confidentiality, and authenticity of the document.

The traditional analog document is created once in object form—a sheet of paper with a surface of designs or letters. The physical parameters of the object are stable with regard to external effects, and any changes made are relatively easy to detect. Over the course of its entire life cycle, the object document is not transformed into a different object. At any moment, the analog document is concentrated in a single point in space, so opportunities for unauthorized access are limited. The selection of available traditional information technologies is narrow, so the requirements for standard technology are obvious in their omission. Electronic documents are another matter. The ease and simplicity of modifying them are based on the very environment in which they exist—copying and replacement operations are fundamental even in Turing machines. The electronic document is transformed many times during its life cycle, and physical indications of its distortion are difficult to find. Here, requirements for the correlations of technologies and standards are extremely significant. Therefore, protecting the electronic exchange of information involves two classes of tasks: ensuring that the document remains equivalent to the original electronic document or standard over the course of its life cycle and ensuring that the electronic technologies used remain equivalent to the standards prescribed by the sector of effectiveness.

In the electronic environment it makes no sense to interpret information as data, sense, knowledge, or fact. Random numbers are also poetry to a computer—a multitude of binary bits, from which comes order, a sequence of 0's and 1's. Any two multitudes reflect the same information if the given relation of order is maintained—there are a multitude of isomorphs.³ Thus, a binary-limited sequence can always be transformed into a number, and in the electronic envi-

ronment, information is a number. A number does not change over time and space but is always fixed and static. When stored on a memory disk, a number is reflected by a “painting” of the disk surface with magnetic domains of various orientations. It is said that a computer’s memory stores data, understood as the fixed form of existence of electronic information: data are numbers.

The purpose of any sort of protection is to ensure the stability (fixation) of the given properties of the protected object in all points of its life cycle. The degree of protection of an object is determined by comparing the standard (the object at an initial point in space and time) with the result (the object at the moment of observation). In our case, at the point of observation (when the electronic document is received) there is only very limited contextual information about the standard (content of the initial electronic document), although we have full information on the result (the document as observed). This means that the electronic document must contain attributes attesting to its compliance with technical and technological requirements, particularly the immutability of the information at all stages of document creation and transmission. One such attribute might be authentication security codes.²

- **Protection of documents during creation.** An authentication security code must be produced on a device basis during the creation of a document. Before code production begins, the isolation of the software environment must be ensured. There must be no opportunity for copying the document onto an external storage disk before the security code is produced. If a document is created by an operator, the code must indicate the operator’s identity. If a document is created by the software component of the automated system, the code must indicate which software component it was.

- **Protection of documents during transmission.** Protection of the document during its transmission over external (open) communications channels must be implemented through the application of certified cryptographic tools, including those involving electronic digital signatures, for every document transmitted. Another option is also possible, in which a packet of documents is signed with an electronic digital signature, and each document is verified with another analog of a handwritten signature, for example, an authentication security code.

- **Protection of documents during processing, storage, and execution.** During these stages, document protection is ensured with the use of authentication security codes, which are required at the start and finish of each stage. These codes must be produced on a device basis and be linked to the processing procedure (the stage of information technology). For an incoming document with an authentication security code (ASC) and electronic digital signature, ASC_2 is produced and only then is the digital signature removed. Furthermore, at the next stage (n), ASC_{n+1} is produced and ASC_{n-1} is removed. Thus, at any moment, the document is protected by two codes— ASC_n and ASC_{n+1} . Authentication security codes must be produced and verified for any document placed in the operating

memory of a computer in which software environment isolation has been established and maintained. ASC_{n-1} is removed after ASC_{n+1} is put in place.

- **Protection of documents during access from the external environment.** When a document is being accessed from the external environment, its protection involves two mechanisms that have already been described above, namely, identification/authentication of remote users and limitation of access to documents, computer resources, and networks.

PROTECTION OF DATA IN COMMUNICATIONS CHANNELS

Channel coders have traditionally been used to protect data in communications channels, and there are no alternatives. Two points must be kept in mind: (1) certification and (2) channels transmit not only data but also control signals.

PROTECTION OF INFORMATION TECHNOLOGIES

Electronic documents in automated systems are not only stored but also processed. A computer represents memory and computation. When a document is processed, some data disappear and others appear, but the information remains the same. The numbers change but the information does not, as the isomorphism is maintained between the multitudes of binary signals in the old and new formats. In the electronic environment, there must be in principle some new form of existence for information accompanying the process of data transformation—information cannot disappear between the start and conclusion of the process. We must therefore assume that information exists in a dynamic form, in the form of a process.

A process is by definition dynamic, involving the changing of something over time, while information must be constant. To avoid a contradiction, a dynamic process must have some time-fixed or static feature. Such a feature exists: the fixation of the description of the process in time, no matter what point in space (a computer) or moment in time the process was observed. In fact, the specific process of information processing in a computer is determined by a fixed algorithm, procedure, or protocol. Assuming there are two forms for representing information in the electronic environment—static, in the form of an object, and dynamic, in the form of a process—we can therefore also assume that there are two fundamentally different classes of elements in the electronic environment. As soon as the first class is defined as numbers, the second class may logically be termed functions (transformations, representations). At the start of a function, we have numbers (data), while at the end, we see new numbers (data). At any moment in time and any point in space, the function remains a function. The function (or in related terms, the representation, algorithm, transformation) is unchanged.

In passive form (storage), an electronic document is a fixed object in an analog environment (memory device), while in an active form, an electronic

document exists as a fixed process in an electronic environment. Accordingly, let us identify two components involved in protection: protection of data (numbers), or the electronic document itself as a physical object, and the protection of processes (functions), representing the active form of existence of the electronic document. Information (data) is defined as a multitude with a specified relation of order. Protection of functions (algorithms) means protection of the computing environment in unvarying form with regard to the information or data processed in it. Electronic technology also represents an ordered multitude (of operations or processes) and therefore can be formally recognized as information technology. The internal unity of the components of protection is revealed: It is protection of information data and protection of information technology. Thus, the status of the document includes not only the identity of the document itself (its compliance with a standard) but also the compliance of the information technologies used with standard requirements.

Despite the obvious similarity, mechanisms for the protection of the electronic document as an object (number, data) and as a process (function, computing environment) are radically different. In contrast to the situation with protection of an electronic document, with protection of information technology, the characteristics of the required technology standard are reliably known, but there is limited information about the compliance with these requirements by the technology actually used, that is, the result. The electronic document itself, or more accurately its attributes, is the only object that could carry information about the actual technology (such as sequence of operations). As before, one such attribute would be the authentication security code. The equivalence of technologies could be established more accurately with a greater number of functional operations linked through this security code. The mechanisms would not differ from those used in protecting electronic documents. Furthermore, the presence of a particular authentication security code could be considered to signify the presence of a corresponding operation in the technological process, and the value of the code could also indicate the integrity of data at a given stage in the technological process.

LIMITATION OF ACCESS TO DATASTREAMS

As a rule, routers with a virtual private network builder function are used to limit access to datastreams. This function may be carried out reliably only with the help of cryptographic tools. In such situations, special attention must be paid to the key system and the reliability of key storage. Naturally, requirements for access policy in the differentiation of datastreams are completely different from those in the limitation of access to files and catalogs. In the latter, only the simplest mechanism is possible—access is either permitted or forbidden.

Complying with the requirements discussed above ensures a sufficient level of protection for electronic documents as the most important type of reports processed in information systems.

NOTES

1. Streltsov, A. A. 2002. Ensuring Russia's information security: Theoretical and methodological foundations. Moscow: Moscow Center for Continuing Mathematical Education, 296.
2. Konyavsky, V. A. 1999. Information security management using the Akkord network security device. Moscow: Radio and Communications Publishers, 325.
3. Gadasin, V. A., and V. A. Konyavsky. 2001. From document to electronic document: Systems fundamentals. Moscow: RFK-Image Lab, 192.

International Aspects of Creating a State System for Countering the Illegal Circulation of Radioactive Materials in the Russian Federation

*Vladimir M. Kutsenko**

Department for the Protection of Information and Nuclear Materials and Facilities, Ministry for Atomic Energy

I have been assigned the task of making specific recommendations for a program of joint activities in counterterrorism. These recommendations are based on practical measures we are taking in the Russian Federation to combat the potential for nuclear and radiological terrorism. Coming from a federal executive agency, our recommendations are of a purely practical nature in accordance with the purview of the Russian Ministry for Atomic Energy (Minatom).

We hope that the following five proposals correspond to the fundamental goal of the conference organizers by focusing specifically on what we should do and how we should do it.

1. On the initiative of Minatom in cooperation with the Russian Ministry of Internal Affairs (MVD), Federal Security Service (FSB), and Ministry of Foreign Affairs (MID), and with the involvement of other interested ministries and agencies, we have developed a draft of a provisional statute on a state system for countering the illegal circulation of radioactive materials within the Russian Federation and across its borders. This draft is being circulated for revision and approval by all relevant entities.

2. The draft statute includes the fundamental conceptual elements necessary for organizing the struggle against the illegal circulation of radioactive materials and for creating a state system linking and organizing the activities of the basic law enforcement and customs agencies, ministries, and departments dealing with the nuclear sector, and other interested organizations. The draft also defines the basic responsibilities and functions of these ministries, departments, and organizations, which primarily lie in preventing the possible criminal use of nuclear materials and radioactive substances.

*Translated from the Russian by Kelly Robbins.

3. To facilitate further consideration of matters related to cooperation among the structural components of the system, plans for the first stage of the project call for creating a model district in the Moscow region as an element of the system for countering the illegal circulation of radioactive materials. A possible structure for such a model district is presented in Figure 1.

4. A fundamental component in the creation of a state system for countering the illegal circulation of radioactive materials is the development of devices for their detection, location, and identification and the provision of such instruments to the structural components of the system. Taking into account the special requirements inherent in the use of such devices, Minatom has created and tested models appropriate for stationary and mobile use. They may be categorized by intended use as follows: (a) handheld gamma and gamma-neutron monitors and similar devices for concealed installation for the detection and location of radioactive materials and (b) portable spectrometric devices for the identification of radioactive materials.

5. The draft statute pays special attention to the question of creating a well-developed information system on matters related to combating the illegal circulation of radioactive materials, including a number of central and agency-specific databases. In creating such systems, Russia also deems it expedient to propose that the international community examine the question of joining forces and coordinating the activities of all interested countries.

The main goal of creating a model district and subsequently implementing other elements of the draft plan is to facilitate the development of a federal system of preventive measures for combating nuclear and radiological terrorism. In this regard, Minatom proceeds from the belief that the problem cannot be resolved through a division of efforts by the various agencies but rather requires federal coordination.

International cooperation in countering nuclear and radiological terrorism is an objective necessity. In this area, there are problems demanding the unification of international efforts and the coordination of activities. In our opinion, these fundamental problems include

- addressing matters related to the detection of nuclear materials
- equipping law enforcement agencies with the necessary technical means and providing general and technical training for their personnel
- dealing with organizational, legal, and other aspects of incident response

In dealing with all these problems as well as other matters, we feel it is necessary to create a joint working group operating under conditions of confidentiality.

We note that any form of terrorism presents a special threat to cities, with even greater consequences in national capitals. In this regard, creating a model

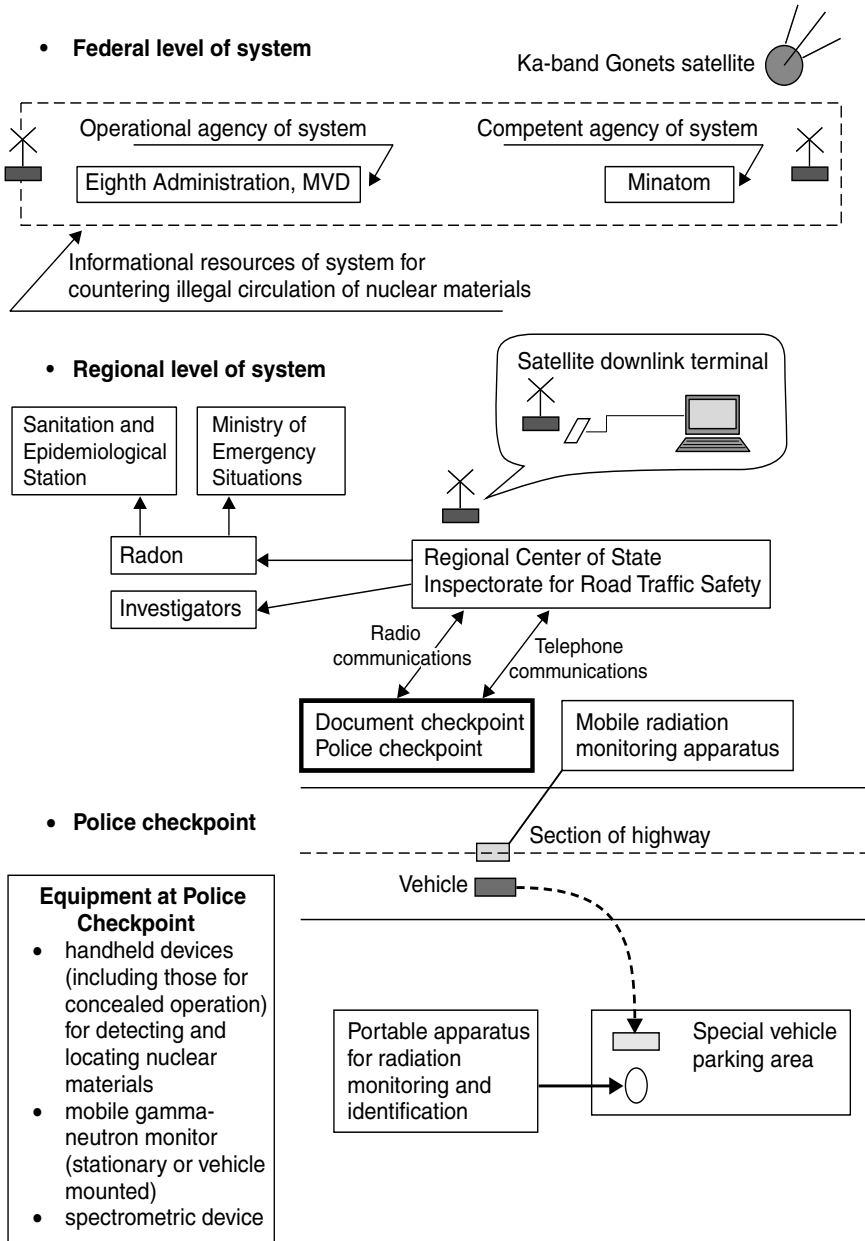


FIGURE 1 Possible structure of experimental district in the system for countering the illegal circulation of nuclear materials.

district in the Moscow region in 2003–2004 and obtaining practical results from its operation will make it possible to formulate a concept (system model) for protecting capital cities, especially those of United Nations Security Council member states, from the threat of nuclear and radiological terrorism.

At the same time, existing technical means for monitoring shipments of explosives, other hazardous cargo, weapons, and so forth, could be brought to bear in the creation of such a system. Work on addressing problematic questions in the model district could add substantial programmatic and practical impetus to efforts to deal with this urgent current problem.

Proposals to the International Atomic Energy Agency (IAEA) of an international program for countering and suppressing the illegal circulation of radioactive materials as a preventive measure in the struggle against nuclear and radiological terrorism could serve as a basis for cooperation. My preliminary estimate is that the establishment of monitoring devices in a model district will cost the equivalent of \$250,000.

It should also be noted that all matters connected with the creation of this system are of a confidential nature and should not serve as instructions to terrorists in how to circumvent it.

Computer Security Training for Professional Specialists and Other Personnel Associated with Preventing and Responding to Computer Attacks

Anatoly A. Malyuk, Nikolai S. Pogozhin, and Aleksey I. Tolstoy*
Moscow Engineering Physics Institute

INTRODUCTION

The level of knowledge and skills required in the area of information security is among the basic factors determining the effectiveness of efforts to counter computer attacks on real targets. Therefore, the training of specialists in this field may be considered one of the most important organizational-technical means of ensuring information security. As noted in the Doctrine for Information Security in the Russian Federation, “the development of a system for training personnel involved in ensuring information security” is among the top-priority measures to be taken in implementing state policy for ensuring Russia’s information security. The training system for information security personnel, for which the foundations have already been created, is one of the most important elements of information security as a whole. This report reviews the characteristics of the information security personnel training system in Russia, defines the basic areas of educational activity, and highlights the most promising of them, which are associated with continuing education. The report also discusses the basic problems that need to be resolved in order to ensure that the necessary level of training is provided for specialists and other personnel at facilities where information technologies could be subject to computer attacks.

*Translated from the Russian by Kelly Robbins.

THE TRAINING SYSTEM FOR INFORMATION SECURITY PERSONNEL IN RUSSIA

Russia has laid the foundations for a state system for training personnel in information security. This system is composed of the following elements:

Training Providers

- higher educational institutions (more than 80) having licenses to educate students in one of seven specialties included in the state classified listing of specialties and areas of training for degreed specialists
 - regional training and scientific centers (22), based at leading higher educational institutions in the various regions of Russia and designed to address problems of providing training for specialists in a specific region
 - continuing education training centers (as a rule, not state run; established in almost all regions of Russia, so it is difficult to determine their numbers), created by organizations actively operating in the information protection services market and licensed to conduct their training activities by local governmental authorities responsible for education

Participants

- university students and other course participants being trained at higher educational institutions, regional training and scientific centers, and continuing education training centers
 - instructors at the various educational institutions and centers
 - administrative personnel organizing and facilitating the training process

Educational and Methodological Resource Support

- state educational standards for higher professional education in the seven specialties included in the information security classification
 - educational plans for training specialists in the specific specialties
 - educational programs for specific training courses in the seven specialties
 - educational programs for continuing education or retraining courses aimed at allowing participants to obtain additional qualifications
 - textbooks, educational and methodological handbooks, and practical laboratory training exercises
 - informational materials supporting the training process

Management Subsystem

- Russian Federation Ministry of Education, which issues licenses for educational activities conducted by higher educational institutions

- executive-branch entities at the regional level responsible for education and the licensing of educational activities associated with continuing education
- educational methodology associations—public organizations composed of representatives of educational institutions that train specialists in the information security field, as well as organizations and departments that employ such specialists (These associations monitor the educational activities of the various institutions and centers to ensure that students are provided with the necessary training at a level meeting the requirements established by the State Educational Standards.)

The two basic types of educational activities being carried out within the system for training information security personnel are as follows:

1. training of degreed specialists: specialist (seven specialties; title: mathematician or information protection specialist; training duration: five or five and a half years); bachelor's degree (four years); master's degree (six years)
2. continuing education: qualification improvement (72 or more training hours); additional qualification (up to 500 training hours); complete retraining (more than 500 training hours)

An evaluation of the need for information security specialists to deal with the problems of countering computer attacks indicates that the first type of training is not meeting all objectives for the following reasons:

- the long duration of training for specialists (up to six years to complete training). The training system that has been created is just getting under way in Russia. It will show its full capabilities once the first six-year training cycle is complete.
- the insufficient number of specialists being graduated. Given the number of higher educational institutions that graduate information security specialists (about 80) and the average number of specialists per year graduating from such institutions (about 20), the average number of specialists graduating each year is estimated at about 1,600. According to several estimates, state institutions alone need to hire about 1,500 such specialists per year, and this does not take into account the needs of the large number of private enterprises and organizations.
- the inertia of the educational process associated with the long-term stability of educational programs and plans (lasting about one training cycle). During this time, the subject matter requirements could change significantly.
- problems of professional orientation for incoming students owing to the difficulty of instituting strict principles for the selection of personnel to be trained in information security specialties. The existing educational system is oriented toward the training of young people, beginning from the first year in

university (age 17–18). Even if a strict system of selection were to be put in place not only on the basis of knowledge but also taking into account psycho-physiological characteristics (and this is very doubtful), effective selection will not be ensured, as during the training period (up to six years) the given parameters could change substantially. Furthermore, young people's life goals are also subject to significant changes. As a result, specialists graduating from these higher educational institutions could either not work in their area of specialization or could carry out functions antithetical to the goals of information security protection.

- difficulty of organizing targeted training for specialists to meet the needs of specific enterprises. Unfortunately, at present it is difficult for any enterprise to define the skills and knowledge that information security specialists will need when they graduate four to six years from now.

This type of educational activity represents only one segment of the training requirements. Information security specialists are commonly employed in the development and creation of complex information protection systems requiring a broad range of knowledge and skills.

In contrast to the training of degreed specialists, continuing education has a number of substantial advantages. These include

- short duration of training (72–500 hours)
- flexibility and possibility of changing educational programs
- ease of implementing targeted training geared to the interests of specific enterprises
- possibility of meeting quantitative needs for trained specialists

Therefore, we might expect that this form of educational activity will find broader application in the training of professional specialists and other personnel involved in combating computer attacks. This activity is oriented toward the utilization of specific information technologies and information protection systems. It would be useful to review the particular features of continuing education in greater detail.

Continuing Education in Information Security

When we account for the problems that arise during the educational process, it is possible to define the special characteristics of continuing education in information security by answering the following questions: “Who should be trained, what should be taught, and how and where should training take place?” “How should the training be managed?” “How should learning be evaluated?” We shall now attempt to answer these questions.

The answer to the question “Who should be trained?” is associated with the selection of the contingent of students. It is appropriate to follow the principle of a differentiated approach aimed at determining the categories of students working at specific enterprises. These categories could include the following:

- information technology specialists working in units responsible for the operation of hardware and software
- specialists who use information technologies in units involved in carrying out an enterprise’s primary mission
- information protection specialists working in information security units
- information security administrators responsible for monitoring the level of information protection
- physical security specialists. Modern physical protection systems are complex automated control systems consisting of devices (microprocessors, video equipment, other special hardware, computers, communications channels and systems) and software (systems software and applications) operated by security service personnel. An automated system of this sort processes “sensitive” information, the loss or distortion of which could reduce the operational effectiveness of the entire physical protection system and, as a result, could help terrorists accomplish their objectives.
 - unit managers
 - senior management

It should be noted that training managers at all levels is a requisite component of personnel training. Knowledge of the basic objectives involved in countering cyberterrorism and of ways of accomplishing these objectives is a mandatory condition for effective decision making both at the stage of creating an information security system and at the stage of responding to a critical situation.

Another point is that functional responsibilities involved with the management of information technologies and those involved with the management of information security subsystems must be divided among various specialists. Because of this requirement, those receiving training should be divided into different groups.

The question “What should be taught?” may be answered through the selection of training programs. The special nature of the professional knowledge and skills of information security specialists combined with the possibility of using such dual-use knowledge and skills for contrary purposes allows us to formulate the following principles that should provide guidance in the selection of training programs:

- Offer a differentiated approach to training, that is, different training programs for different categories of students.

- A specialist should have only the knowledge and skills he is supposed to have. Extra knowledge and skills could lead the specialist to develop ambitions that could lead to his carrying out unauthorized operations on his own initiative or under the influence of an outsider. The consequences could be catastrophic. Consequently, extra knowledge and skills among information security specialists could be harmful, and this must be kept in mind in designing training programs. Representatives of the enterprises whose employees are being sent for training must therefore play an important role in the program design process. This will help to ensure that the continuing education programs are targeted to the specific needs of the enterprises.

- Establish authorized access to the educational content. Given the nature of the knowledge and skills possessed by information security specialists, this sort of knowledge should be conveyed only to those who need it. Students are selected solely by the enterprises sending personnel for training. This also helps to ensure the targeted nature of extended training programs.

- Ensure the information security of the training system. This principle follows from the preceding one. The training system must ensure the accessibility, confidentiality, and integrality of information needed for the educational process (primarily with regard to the material covered in training).

Answering the question “How should training take place?” makes it possible to define the technological requirements involved in implementing continuing education programs. Most training centers in Russia generally use traditional educational technologies (lectures, seminars, practical exercises), which require that students take time off from work to participate. The development of the system for training information security personnel is oriented toward the use of modern information and educational technologies. This makes it important for the educational system to introduce distance-learning technologies such as virtual training courses, electronic textbooks, and remote testing. This should increase efficiency and reduce training costs because of a reduction in the amount of time required for training (trainees spend less time away from their worksites).

The answer to the question “Where should training take place?” is already determined in the given case. At present, it can be stated that the necessary facilities for the information security training system have already been established, as described above. The further development of these facilities entails the resolution of such problems as how to improve methods for their management, how to ensure the information security of the training process, and how to develop their material and financial infrastructure.

Improving and developing the personnel training system in the information security sphere requires a response to the question “How should training be managed?” Here, it is necessary to look at the prospects for the development of

the training system itself, taking into account the key points involved in implementation of the Federal Targeted Program for the Development of a Unified Educational Information Environment (2001–2005), which was enacted by Resolution 630 of the Government of the Russian Federation dated August 28, 2001. This program calls for the “creation of conditions for a phased transition to a new level of education on the basis of information technologies. . . .” Therefore, the system for personnel training in information security must be viewed as part of the unified educational sector of Russia, understood as “the totality of organizational measures, informational and methodological resources, and modern educational and information technologies that ensure the high quality of education in all regions of Russia and the effective utilization of the country’s scientific and pedagogical potential.” Consequently, management of the modern personnel training system for the information security sphere must take into account the following points:

- standardized educational and methodological resources
- existing infrastructure of system facilities
- availability of modern information and educational technologies in the system
 - existence of a tri-level system for the management of education in Russia (Ministry of Education or Regional Administrative Agency—Educational Methodology Association—Educational Institution or Training Center)
 - need to protect information presented in course content

It therefore follows that the system for training information security personnel must look like a corporate training system meeting the need to provide training for specialists within defined limits, for example, the need to ensure information security, and this must be taken into account in managing such a system.

The answer to the question “How should learning be evaluated?” carries with it additional changes in the management of the system for training information security personnel. The nature of the knowledge and skills possessed by information security specialists gives rise to the need for adherence to the following principles in evaluating the level of learning among students:

- standardized approach to the certification of specialists completing multiyear courses at higher educational institutions
- differentiated approach to certification of specialists completing continuing education courses

This involves

- testing of knowledge at the end of a specific course of study completed at an educational institution or center

- certification of a given level of knowledge and skills by an independent certification center
- certification of knowledge and skills meeting current job requirements at the student's worksite (could be conducted by a unit or senior staff at the worksite in cooperation with training or certification centers)

Implementing the measures outlined above entails subsequent changes in the system for managing personnel training in the information security sector:

- improvement of the testing system
- creation of the two types of certification systems described above

The requirements of the system for training information security personnel, taking into account the field of continuing education, are based on the experience of the Moscow Engineering Physics Institute (MIFI).

TRAINING OF INFORMATION SECURITY SPECIALISTS IN THE DEPARTMENT OF INFORMATION SECURITY AT MIFI

MIFI has been involved in educational activities in the information security field since 1991. Degree programs are offered for specialists in the fields of comprehensive protection of information technologies and comprehensive information security for automated systems. Graduates of these programs are qualified as information protection specialists, and the course of study takes five and a half years to complete.

Continuing education is provided in the form of qualification enhancement courses. The educational programs are different for the various categories of students and are coordinated in advance with the organization sending students to be trained, taking into account their individual requirements. MIFI's leading partners (clients for educational services) in the realm of continuing education for information security personnel are the Central Bank of the Russian Federation and the Savings Bank of the Russian Federation. The educational technologies used are both traditional (with students taking time off work) and modern, involving elements of distance-learning technologies (with students spending only part of their training time offsite). Between February 1995 and December 2002, more than 2,500 specialists from all regions of Russia have been trained.

Examples of the continuing education training programs being conducted by MIFI in 2003 are presented in Table 1.

COMMUNICATIONS ACTIVITIES

Experience and information on teaching methodologies in the information security field are shared at conferences at various levels. The following confer-

TABLE 1 MIFI Continuing Education Programs

No.	Program	Training duration, hours/days
<i>Training Cycle 1: Security of Bank Information Technologies</i>		
1.1	Security of network technologies	88/11
1.2	Protected corporate bank networks	40/5
1.3	Information security of bank e-mail systems	40/5
1.4	Security of bank intranets and virtual private networks	40/5
1.5	Cisco Systems solutions for protecting corporate information networks	40/5
1.6	Systems for detecting attacks on corporate bank networks	24/3
1.7	Monitoring network security	40/5
1.8	Anti-virus protection for information technologies	24/3
<i>Training Cycle 2: Administration of Information Technology Security</i>		
2.1	Information technology administrators	40/5
2.2	Administering corporate virtual private networks using FPSU-IP screening routers	40/5
2.3	Information security in a Microsoft Windows NT environment	40/5
2.4	Information security in a Microsoft Windows 2000 environment	40/5
2.5	Information security in an OC Sun Solaris environment	40/5
2.6	Data security mechanisms and policies in SQL	24/3
2.7	Data security mechanisms and policies in Oracle	24/3

ences are held annually under the aegis of the Ministry of Education of the Russian Federation:

- Problems of Information Security in the Higher Education System (January, Moscow, MIFI)
- Information Security (including international participants; June, Taganrog, State Radiotechnical University)
- Methods and Technical Means of Ensuring Information Security (October, St. Petersburg, State Technical University)

At the international level, efforts to develop systems for training information security personnel in various countries are coordinated by Working Group 11.8 (Information Security Education), which is part of Technical Committee 11 (Security and Protection in Information Processing Systems) of the International Federation for Information Processing. The World Conference on Information Security Education (WISE) is held every other year with the support and direct participation of this organization. The third such conference, WISE-3, will be held in the United States (Monterey, California), June 26–28, 2003, and WISE-4 is scheduled to take place at MIFI in Moscow in May 2005.

Medical Aspects of Combating Acts of Bioterrorism

*Gennady G. Onishchenko**
Russian Ministry of Health

The national strategy for health protection against infectious diseases must also take into account the problem of combating bioterrorism, a problem that is the focus of increasing attention on the part of the government, the public, and specialists in many countries. Underestimating modern biological capabilities and the dangers they entail could have a disastrous impact on the national security of the state.

The imperfect nature of mechanisms for monitoring compliance with the chemical and biological weapons conventions, suspicions regarding the continuation of work on biological weapons programs, and a number of incidents involving attempts to intentionally use biological agents for terrorist purposes are evoking serious concerns that terrorists might actually use biological means as weapons.

One of the first and most illustrative examples of the use of bioterrorism was the intentional poisoning of residents of a small city in the state of Oregon (United States) in September 1984 by means of adding *Salmonella typhimurium* to the salad dressing at 10 of the city's most popular restaurants. The aim of this action was to cause a massive number of food poisoning cases and thus affect the outcome of local elections according to the interests of representatives of a cult sect. Two points are worthy of note. First, officials investigating the mass poisoning incident took a year to determine that the *Salmonella* had been introduced by terrorists. Second, the American authorities prohibited any information about this incident from being published for 12 years because of their concerns that it might serve as an example for other extremists throughout the country.

*Translated from the Russian by Kelly Robbins.

Other subsequent cases involving the attempted use of biological agents for terrorist purposes have triggered a flood of publications and numerous scientific conferences and have spurred many countries, especially the United States, to institute many legislative, legal, organizational, medical, and other measures aimed at countering bioterrorism. The United States has devoted substantial sums to the problem of fighting bioterrorism, including on matters of “internal preparedness,” inasmuch as expert analyses, evaluations, and inspections have led to the conclusion that in most cases, public service agencies are not prepared to respond to terrorist attacks involving the use of biological weapons. Efforts are under way to implement a program to develop and create stockpiles of 18 new vaccines, including a new smallpox vaccine. In addition, funds have been allocated to create a stockpile of medicines and antibiotics, which are intended primarily for use by police, fire, and emergency medical personnel. Appropriate attention is being focused on the fight against terrorism in Russia as well. The Interagency Antiterrorism Commission was created in 1997, the State Duma passed the Law on Combating Terrorism in July 1998, and the Government of the Russian Federation issued a resolution establishing a federal targeted program in 1999.

Although many countries have well-prepared systems for combating ordinary terrorism and dealing with emergency situations (floods, earthquakes, accidents, and catastrophes), none has put in place a complete set of measures for meeting this new threat. This is because for many reasons it is extremely difficult to combat the use of biological agents for terrorist purposes (the large number of potential agents, the long incubation period, the lag time before symptoms of illness appear, the possibility of secondary infection and the further spread of the disease, and so forth).

Medical personnel must also play a special role when bioterrorist acts are carried out. They must understand the epidemiological situation and know the potential biological agents and the symptoms of the infectious diseases they cause, which as a rule would differ from those of naturally occurring illnesses. They must also be aware of treatment protocols and measures for preventing the spread of epidemics. However, the current state of affairs is such that most clinical microbiological laboratories have neither the capabilities nor the experience in real-life detection and identification of infectious agents from a list of those that might be used by bioterrorists, such as anthrax, brucellosis, botulism, cholera, plague, smallpox, hemorrhagic fever viruses, and others.

Biological agents of critical importance from the standpoint of civilian public service preparedness may be divided into the following three categories based on their characteristics:

1. Category A

- smallpox (*Variola major*)
- anthrax (*Bacillus anthracis*)

- plague (*Yersinia pestis*)
- botulism (*Clostridium botulinum*)
- tularemia (*Francisella tularensis*)
- hemorrhagic fevers (filoviruses, arenaviruses, and so forth)

2. Category B

- Q-fever (*Coxiella burnetii*)
- brucellosis (*Brucella spp.*)
- glanders (*Burkholderia mallei*)
- melioidosis (*Burkholderia pseudomallei*)
- viral encephalitis (Venezuelan equine encephalitis, Western equine encephalitis, Eastern equine encephalitis, and so forth)
- typhus (*Rickettsia prowazekii*)
- psittacosis (*Chlamydia psittaci*)
- foodborne agents (*Salmonella spp.*, *Shingella dysenteriae*, *E. coli 0157:H7*, and so forth)
- waterborne agents (*Vibrio cholerae*, *Cryptosporidium parvum*, and so forth)

3. Category C

Newly emerging agents (antibiotic-resistant bacteria and tuberculosis, Nipah virus, AIDS, and so forth)

Without denying that health care institutions respond rather adequately to naturally occurring infectious disease outbreaks, it must be noted that a significant proportion of the methods currently used in Russia to identify pathogens do not meet the necessary standards for identifying biological agents that are used intentionally. These methods have become outdated and are unsatisfactory primarily from the standpoint of the time required to use them.

The system of scientific, organizational, and other measures aimed at improving the preparedness of the health care system for meeting the threat of bioterrorism must not undermine the measures already in place to combat infectious diseases. Instead, it should promote the constant improvement of the health care and biomedical research infrastructure and facilitate cooperation involving the capabilities of other agencies, such as the Ministry for Emergency Situations, regional units of the sanitary-epidemiological service, and relevant scientific research institutes. The most important measures to be taken in improving these efforts would include the following:

- The major regional centers, especially those with international airports, should have permanently operating infectious disease hospitals equipped to at least the P-3 biosafety level.
- These hospitals must be amenable to continuously improving their methods for treating infectious diseases, up to and including being willing to participate in clinical trials of new drugs and actually doing so.
- Regional clinical microbiological and immunological laboratories are also needed, and it is important that they be fully operational according to the highest modern standards. They should be associated with the infectious disease hospitals mentioned above and should be equipped to at least the P-3 biosafety level.
- These laboratories must be open to new technologies and methods of identifying, diagnosing, and deactivating infectious agents, and in this regard, they must support close linkages with the relevant scientific research institutes working in the given field.

The following actions should be taken as part of the Federal Scientific Research Program on Combating Bioterrorism:

- Develop new express immuno-enzyme and other test systems for detecting antigens and antibodies as markers for hemorrhagic fever viruses, smallpox, anthrax, tularemia, plague, legionellosis, malaria, and so forth.
- Develop various types of polymerase chain reaction (PCR) diagnostic tests, including those using biochip technology, for express diagnosis and detection of pathogens within a few hours or even minutes.
- Establish modern, well-equipped PCR laboratories in various regions of Russia.
- Conduct additional research on the pathogenic characteristics of especially dangerous infectious agents and search for new medications for treatment and emergency prophylaxis of individuals infected with these agents.
- Develop vaccines against infectious agents for which none yet exist or for which existing vaccines are inadequately effective or unsatisfactory for other reasons.
- Provide specialized training for medical personnel and laboratory workers in safe methods for handling, analyzing, and detecting such agents in research centers and clinics with real experience in this area.

Efforts in these areas will not only bring real results in the struggle against bioterrorism but will also improve the health care situation in general.

Certain Aspects Regarding the Development of Conditions Favorable to Cyberterrorism and the Main Areas of Cooperation in the Struggle Against It

Igor A. Sokolov and Vladimir I. Budzko*

Russian Academy of Sciences Institute for Informatics Problems

The concept of cybernetic terrorism is interpreted rather broadly. In order to work out the necessary approaches for preventing threats of unauthorized penetration of systems—intrusion and infliction of damage—we believe it is appropriate to consider the problem from the standpoint of ensuring computer security. In doing so, it is simplest to classify the various types of intruders according to the goals of their actions, for example,

- obtaining access to secret data
- altering data that affect the completion of processes (within a particular automated system or outside it, but under its control) in which the perpetrator has an interest
 - vandalism
 - informational impacts, for which specific individuals or groups behave according to the perpetrator's wishes

The capabilities offered by modern information technologies for data storage and transmission may also be used for the hidden exchange of information to provide support for illicit activities. Thus, there are two main types of illegal activities in the computer sphere:

1. unauthorized penetration or intrusion into a computer system
2. hidden transmission of data via legal channels

*Translated from the Russian by Kelly Robbins.

Let us look first at external intrusion, that is, unauthorized penetration by perpetrators through devices to which they have free access. We will devote separate attention to threats from personnel within a given system on the supposition that the necessary organizational and other security measures have been put in place.

In the early 1980s, intrusion received a certain amount of attention in systems where state and corporate secrets were stored. Here, the focus was primarily on limiting the access of end users to information stored in a system. The question of security for physical data carriers was handled rather simply, mainly through organizational measures.

Information security was based on the principle of creating conditions in which the user has no physical opportunity to make any changes in the software programs—nonprogrammability. It was implemented by means of so-called dumb terminals and classical operating systems (IBM, DEC, and others), the architecture of which involved the separation of programs and data and the physical protection of systems software from applied programs and other elements. Furthermore, communications technologies were systems oriented and did not permit outsiders to log on. Exchange protocols for the telecommunications components did not allow perpetrators to penetrate the network.

The level of security provided by the architectural characteristics of computers and communications devices was sharply reduced with the appearance and accelerated introduction of new technologies, of which the following deserve special attention:

- personal computers, especially IBMs using Microsoft operating systems
- local networks with personal computer (PC) workstations
- the transmission control protocol/Internet protocol (TCP/IP) family of protocols and the creation of the Internet on their basis

A keen struggle began among the various means of protection and attack. The first applications for PCs were for home use. Within a few years, PCs began to be used in almost all spheres of human activity. IBM-compatible PCs using Microsoft software established a dominating position. With their simplicity of use and relatively low cost, they made it substantially easier and less expensive to create small systems for various applications than did computers with different architectures. The local nature of their installation made it easy to handle security matters.

This initial period saw the appearance of the first danger signals—computer viruses. At first, the intrusions were destructive in nature. The thesis was advanced that “he who takes careful precautions will not be affected.” Therefore, most of the efforts were focused on the correct use of antivirus software and the proper way to use diskettes. From a security standpoint, it is unforgivable that very little attention was devoted to the operating system architecture and floppy

disk technology serving as the catalyst for the development of intrusion tools. In the development of the architecture to date, almost no fundamental and reliable barriers have been put in place against virus attacks.

In the first stage, virus attacks composed the technology for intrusion. Modern antivirus packages (for example, the Kaspersky antivirus programs) essentially reflect the level of the current intrusion intellect on the whole. When we give high marks to the quality of current antivirus programs, we tacitly give the same high marks to this malicious intellect.

The appearance of local computer network technology laid the foundation for a new stage in the use of PCs. Users were given a qualitatively new interface, convenient and easy to use, which they quickly preferred over previous systems based on dumb terminals. The practical implementation of “paperless information technology” in an organization’s work became a reality. Ethernet gradually became the dominant local network architecture.

The well-protected architectures offered by such manufacturers as IBM and DEC in their mainframe and personal computers were gradually pushed aside. The market supported cheap hardware, and its components became the de facto standard. At the same time, local networks created new channels for intrusion. Their use opened up opportunities for inflicting damages on a substantially larger scale than possible in attacks against a single-user PC. It is very important to note that software carries the majority of the load in organizing the exchange of data over local networks. If there is an intrusion into any PC on the network, the network driver and its network map can be altered, which at a minimum will bring down the entire network.

So-called software agents began to be widely used in local networks to carry out certain functions. These agents are loaded into client PCs in the process of performing a particular function. This approach gained widespread use in the implementation of software for electronic libraries, for which CD-ROMs were used as basic information carriers. Software agents also began to be used in diagnostic and monitoring systems. They appear automatically on specific workstations. For example, electronic libraries that perform essential service functions involved in working with data include an internal search system and other programs that are loaded automatically during disk initialization.

The placement of such a library on a server requires that the appropriate programs be transferred to a client machine. During the transfer process, someone could catch such a program and attach an intrusion program to it. One way of doing this, although it would not be easy, would be to intercept all Ethernet messages on a client machine through a network card configured to receive all MAC addresses. Including codes necessary for intrusion in a program being transferred would ultimately make it possible to gain unauthorized access to another workstation.

Another example of intrusion is the use of WinWord text editor macros. As macros are built-in programs, the addition of intrusion programs in the “body” of

macros makes it possible to distribute them along with text documents and launch them when the text editor begins processing. There are many examples in which WinWord has been used in virus attacks.

Perpetrators have found even broader opportunities in the Internet environment. The dominant position of the TCP/IP family of protocols and their inherent capabilities have given rise to a new wave of various types of attacks with even more destructive consequences. Experience amassed in previous stages and the scientific-technical potential involved in carrying out intrusions has been put to full use.

A stable trend has been established by which the number of Internet intrusions has been doubling each year. This means that the amount of damage done has at least doubled as well. The scope of virus attacks is such that the network space of several countries at once can be affected.

At the same time, the Internet continues to play an increasingly important role as an international information repository and the least expensive means of communications. It is essentially one of the most important engines of world technological progress. It is very important to note that it has become the main daily working tool and information source in a number of fields. One example would be research and analytical activity using accessible electronic information resources via Internet Open Source Solutions, something a growing number of firms and organizations are doing.

In the environment described above, creating an IBM PC-MS-Ethernet-Internet system capable of ensuring the necessary level of security requires the involvement of the necessary number of high-class specialists in the information technology field and the acquisition of expensive security software and devices. The cost of these security technologies for a system built on this platform and requiring a high level of protection equals up to half the cost of the entire system itself. Operating and maintaining the security technologies entail substantial additional costs.

The more well-known outside intrusions that occur, the greater the demand for the products of companies that specialize in creating technologies for information security at various levels and with various purposes, producing methodological materials, and providing security consulting services. This business is developing successfully.

A system that is sufficiently protected from the outside remains vulnerable to intrusions launched from within through the capabilities of service personnel (operators, administrators, systems programmers, security officers, and so forth). A lack of on-staff capabilities in security software development must be rectified by using additional specialized software products from firms that specialize in providing enhanced protection in a Microsoft environment and by instituting additional heightened (and therefore expensive) organizational security measures.

Certain successes have been achieved in the development of technologies for intrusion detection, particularly in the Internet environment. There have been

many more successes in detecting intrusions than in preventing such intrusions. Each time it has released the latest version of its operating system, Microsoft has announced the substantial expansion of the program's built-in security features, but each time it has turned out that these new features do not save average users, who lack the system enhancement capabilities of organizations. The well-known problems of ensuring security in modern automated systems in an IBM PC-MS-Ethernet-Internet environment are also applicable to a significant extent to cases involving the use of the UNIX operating system and RISC (reduced instruction set computer) processors.

New security solutions for virtual private networks (VPNs) have been widely developed in the past few years. The use of VPNs provides substantially increased protection against system intrusions over the Internet but does not resolve the problem within the system itself. VPN technology cannot be used for access to various general-access servers, search systems, portals, other information resources, or electronic mail. Furthermore, as the service provider plays a fundamental role in the organization of a VPN, this requires that these providers be highly responsible and that users place a great deal of trust in them.

Therefore, the first conclusion that can be drawn is that the IBM PC-MS-Ethernet-Internet environment, which is the most widespread today and is used in creating automated information support tools for various functional purposes, is poorly protected against intrusions. Efforts to stop the growth in the number of intrusions have not been successful. This situation is advantageous for firms specializing in the sale of consulting services and the production of supplemental means of protection, such as firewall systems, security shields, and monitoring systems. But it also increasingly complicates the lives of end users. The fundamental reason for this state of affairs lies in the inherent characteristics of the systems architectures. At the same time, the IBM PC-MS-Ethernet-Internet environment still represents the dominant foundation for existing and newly created automated information support systems.

The new technology of dense wavelength division multiplexing (DWDM), in which all types of channels are collocated on one fiber, has seen very rapid development in recent years. Each subchannel has a carrying capacity of 10 GBps, and there are 256 subchannels in each channel. Efforts are continuing to increase the number and carrying capacity of the subchannels. The use of DWDM technology makes it more efficient to use IP as the basic exchange protocol, and this explains the gradual shift away from lower-level protocols such as asynchronous transfer mode (ATM), frame relay (FR), and others.

The use of DWDM in developing the Internet will facilitate a substantial expansion in the volume and content of services provided, including IP-telephony, IP-video, video conferencing, and so forth. These and other types of services will make up an ever-increasing share of overall Internet use. DWDM offers expanded capabilities for making systems disaster resistant, which is defined as the ability of a critical application to maintain vitally important data

and software resources and continue performing its functions (possibly with certain limitations) under conditions of overall system degradation caused by the massive destruction of system components or entire hardware complexes and linkages between them as a result of natural disasters, industrial accidents and catastrophes, or the intentional actions of individuals or groups. This function is also conveniently carried out over the Internet, as in such circumstances it is simpler and less expensive to resolve the problem of rerouting communications channels.

Finally, the use of DWDM makes it possible to advance efforts to implement distributed parallel computing (grid program [peer-to-peer computing]). The Internet is advantageous in this regard as well. Dealing with issues of providing security for data processing and transmission in cutting-edge distributed computing architectures is of fundamental importance if these architectures are to be broadly disseminated and used. The basic security components must provide a mechanism for authentication, access limitation, and confidentiality of communications among elements of the network. Ensuring the integrity of data and processes during failures and catastrophes should also be viewed as an important element of ensuring security. In addition, any system operating in an IP VPN environment must have a subsystem for security management that is designed to ensure the reliable and uninterrupted functioning of the base system in the event of threats or other actions, protect the technological process as a unified whole, and provide monitoring and audit capabilities.

Therefore, our second conclusion is that the Internet will develop and be used on an increasing scale in various spheres of human activity. However, if the IBM PC-MS-Ethernet-Internet architecture maintains its dominance, we will also see an increase in damages from intrusions and especially from intrusions for terrorist purposes.

This leads to our third conclusion, namely, that the danger of computer terrorism can be reduced only by using new systems technology solutions for the design of operating systems, collective use systems, and telecommunications protocols. The following could be suggested as areas for joint research with our American colleagues:

- definition of design principles and implementation mechanisms for ensuring the security of the LINUX operating system and preventing intrusions into individual computers and collective use systems, including the construction of such systems on narrow client principles
- definition of areas for improvement and development of recommendations on changing the IP protocol
- study of questions related to the construction of virtual private networks that are reliable in preventing intrusions
- study of questions related to the implementation of distributed parallel computing (GRID system)

It would also be appropriate to join forces to prepare the necessary methodological materials explaining the practical expediency of intrusion-resistant architectures to stimulate market interest in the shift to using hardware and software that could form the basis for the creation of reliably protected systems. Finally, it would be expedient to work together on preparing well-honed recommendations on the creation of a standardized set of laws on cyberterrorism.

The Role of the Russian Ministry of Internal Affairs in Combating Terrorism in Urban Conditions

*Sergey A. Starostin**

All-Russian Scientific Research Institute of the
Russian Ministry of Internal Affairs

“We are entering a unique era of terrorism that could make all of modern society its potential victim.” These words, spoken more than 20 years ago by Joseph Alexander, head of the Institute of International Terrorism of the State University of New York, are being confirmed in full measure today.¹ The events of September 11, 2001, in the United States and the bombings of apartment buildings in September 1999 and seizure of hostages in October 2002 in Moscow have already firmly convinced everyone that for modern society, terrorism has become a global threat, along with other various dangers to which mankind is subjected at the start of the third millennium.

Indeed, modern terrorism is taking on new forms and features shaped by fast-moving processes under way in the high-technology sphere. Scientific and technical progress is giving rise to new varieties of terrorism. The appearance of such new concepts as biological, chemical, informational, radioelectronic, and environmental terrorism is no mere coincidence.

The globalization of terrorism is evident in that it is the topic of discussion at numerous annual international conferences, an example of which is ours here today. Allow me to thank its organizers for inviting representatives of the Russian Ministry of Internal Affairs (MVD) to take part.

It would be a mistake to think that modern terrorism in Russia in all its most radical manifestations is the result solely of the reform of the previous state socio-economic system and of the processes that have occurred in our country in recent years. Even in “stable” Soviet times, terrorist acts of rather broad impact were carried out in Russia. It is sufficient to recall the bombings in the Moscow subway

*Translated from the Russian by Kelly Robbins.

system in the winter of 1978. This was our first encounter with political terrorism, when the criminals aimed not only to attract attention to themselves but also to kill as many people as possible. The number of victims at that time was in the dozens.

The next stage of radical manifestations of extremism concerns the most recent phase of Russian history. Following is an incomplete list of crimes committed in Moscow alone in the past five years that are classified as terrorism according to our laws:

- 1998: bombings at the Tretyakovskaya subway station (three wounded) and at a synagogue
- 1999: car bombings at the U.S. embassy and the Russian Federal Security Service (FSB) (2 wounded); bombings in the lobby of the Intourist Hotel (11 wounded), at the MVD, and at the shopping mall at Manezh Square (1 killed, 40 wounded); bombings of two apartment buildings on Guryanov Street and Kashirskoe Shosse (more than 200 killed, including 21 children)
- 2000: bombing in the underground pedestrian passageway at Pushkin Square (7 killed, 53 wounded)
- 2001: bombing at the Belorusskaya subway station (10 killed)
- 2002: detonation of a 122-mm fragmentation mine shell at a McDonald's restaurant (1 killed, 7 wounded); seizure of hostages at the theater on Dubrovka Street (129 killed, of which 7 were foreign citizens)

To this list of terrorist acts we should also add the bombings in Buinaksk and Volgodonsk, the bombing of the government building in Grozny, and others. Clearly, this situation in Russia and in our major cities is directly linked with processes under way in the south, especially in the Chechen Republic. This region is also the focal point of the majority of crimes of a terrorist nature.

In predicting how the situation will develop, we should anticipate an increase in terrorism and certain directly associated crimes such as banditry. The increase in the number of serious and extremely serious crimes is a matter of considerable concern. The proportion of these crimes could reach 54.7 percent of all acts subject to criminal penalties. Insufficient sample size precludes us from making a reliable quantitative forecast for the crimes mentioned above. However, current growth trends point to the growing terrorist danger facing all citizens of the country (see Table 1).

During the forecast period, the unbreakable criminological linkage between terrorism and crimes related to the illegal trade in narcotics and powerful psychotropic substances is evident. If the main channels through which drugs flow are not blocked, the volume of drug-related crime will increase substantially. We can expect that the registered number of drug-related crimes will grow by 26.3 percent in 2003 as compared with the level in 2002.

Making a fundamental assessment of the growing crime threat, Russian Federation President Vladimir V. Putin said: "We are paying a heavy price both for

TABLE 1 Crime Forecast for 2003

	2001	Growth (percent) 2002	2003 (forecast)
Worst-Case Scenario			
Banditry	-9.4	-13.1	26.5
Terrorism	142.2	10.1	30.6
Moderate Scenario			
Banditry	-9.4	-12.5	11.6
Terrorism	142.2	15.3	19.0
Best-Case Scenario			
Banditry	-9.4	-13.1	-3.2
Terrorism	142.2	10.1	7.5

the weakness of the state and for the inconsistency of our actions. Meanwhile, I would like to note and to emphasize that Russia will not make any deals with terrorists and will not be subjected to any sort of blackmail. International terrorism is becoming more brazen and operating in an increasingly savage manner. Terrorists are issuing threats to use means comparable to weapons of mass destruction. With a deep sense of responsibility, I would like to state that if anyone even attempts to use such means against our country, Russia will respond with measures adequate to meet the threat to the Russian Federation."²

The threat presented by terrorism to all of civilization has already been recognized at the international level, and there are no grounds on which to expect that this threat will weaken or diminish anytime soon.³ Moreover, the intensification of the terrorist threat to Russia has given rise to the need to make well-founded changes in the national security strategy, specifically with regard to the possible use of the armed forces to eliminate hotbeds of international crime.⁴

The defining characteristic of the current operational situation in Russia is not only the reality that terrorist acts are being committed but also the constant threat that they will be carried out in the future. Here are a few examples. In the fall of 2002, Chechen fighters from the city of Urus-Martan and the village of Vedeno planned a terrorist act that was to be carried out in the city of Volgograd. The dam at the Volzhskaya State Regional Electric Power Station was selected as the target for sabotage. The terrorists planned to purchase explosives from Chechen servicemen in military units. The Chechen diaspora collected funds for this purpose. On August 26, 2002, internal affairs agencies received operational information on the planned terrorist act, which allowed them to prevent it from being carried out.

On October 28, 2002, after the seizure of hostages at the theater on Dubrovka Street, the district department of internal affairs received information that there were 24 men and 6 women (representatives of Arab countries) in Moscow illegally who were involved with the commission of the terrorist act.

It was also established that they intended to depart for the cities of Volgograd, Astrakhan, and Saratov in the near future to organize and carry out terrorist acts there as well.

The flow of such information is not diminishing so far in 2003. We respond immediately to all calls from citizens (up to 500 per month), and we investigate them all, including false reports. These investigations involve onsite work not only by personnel from the local district internal affairs agencies but also by specialists from the field engineering unit and canine teams to check for the possible presence of explosives, bombs, and poisonous substances in unattended or suspicious objects.

During the operations in 2002, we discovered 10.5 percent more crimes punishable under Statute 222 of the Russian Federation Criminal Code (illegal acquisition, distribution, sale, storage, shipment, or possession of weapons, ammunition, or explosive substances or devices) than during the same period of the previous year. In Moscow alone, about 1,000 firearms were taken out of illegal circulation, more than half of them rifles, as well as several hundred military grenades and more than 10 kg of explosives.

It should be noted that the increased criminal-terrorist threat throughout Russia has for the first time presented society with the question of how to minimize the consequences of terrorist acts for the civilian population. This is primarily a matter of prevention and immediate assistance to victims, deactivation of any devices or agents used, development of new means of protection, and education of the public in how to behave safely in terrorist threat situations.⁵

On the topic of preventing terrorism, it is impossible to overlook those important factors that in our view not only destabilize the operational situation in the country as a whole and in Moscow in particular but also give rise to crimes of a terrorist nature. The activities of extremist organizations and groups represent a serious factor in destabilizing the criminal situation in the country. This matter is especially urgent for our capital: There are more than 120 nationalities living in Moscow, people of the most varied political and religious convictions (more than 5,000 Chechens, more than 2,000 immigrants from Dagestan and Ingushetia).

Each day, about 3 million people pass through the capital. On average days, approximately 100,000–150,000 vehicles pass through state road inspection checkpoints on entering the city. Up to 165 long-distance trains arrive at the capital's nine railway stations each day, along with up to 1,950 local trains.

There are more than 300 associations and religious denominations actively operating in the city, and by no means are all of them devoted to pacifist aims. According to our data, more than 1,000 religious groups and cults are conducting their destructive activities in Moscow, preaching fanaticism based on distorted spiritual and ethical canons (the Satan Society, White Brotherhood, Aum Shinrikyo, Jehovah's Witnesses, the Castrati, and many others). It should be noted that a number of religious structures are largely financed by extremist-oriented foreign organizations.

Extremist organizations of a radical political orientation are also operating in the city, such as the People's National Party, Russian Master, the Freedom Party, numerous groups of soccer fanatics, and so forth. The dangers presented by right- and left-wing political extremism should not be underestimated, nor should those arising from the most aggressive form of religious extremism, Wahhabism. These dangers must be evaluated realistically and adequate measures taken in a timely manner to suppress illegal activities.

Here again, it is of primary importance to coordinate the efforts of law enforcement, other government agencies, and various public associations empowered to deal with this problem. Passed in July 2002, the Federal Law on Countering Extremist Activity established the legal and organizational foundations for this activity and delineated the responsibilities of the agencies charged with its implementation.

It must be noted that in the Russian Federation there is a division of functions in the effort to combat manifestations of terrorism. Countering political terrorism falls within the purview of the Federal Security Service, while suppressing criminal terrorism is the responsibility of the MVD.

The MVD is pursuing a number of preventive measures to fight terrorism. Among the most effective are targeted preventive search operations (such as Vortex-Antiterror) aimed at locating individuals belonging to criminal groups of an extremist or terrorist orientation, members of illegal armed groups and their accomplices, and members of Muslim organizations and religious centers that are promulgating Wahhabism.

Terrorism prevention efforts are under way daily and involve almost all the various service units of the MVD. Joint work is being carried out with Moscow's municipal services agencies to seal off garrets and basements of apartment buildings and to check out rented apartments and other facilities in such buildings. Special attention is being paid to protecting and providing operational coverage for the city's industrial sites and other facilities presenting a heightened danger.

An algorithm of actions aimed at preventing terrorist acts and other extremist manifestations in locations where large numbers of citizens gather during major cultural events has been developed and is being applied in practice. The safety program designed for Moscow sports facilities during 2003–2006 calls for the acquisition and installation of modern video observation and monitoring systems, radio and cable communications hardware, and other means for technical control and examination. The total cost of the necessary equipment is 100 million rubles (\$3.28 million).

Units serving the Moscow subway system have also received orientation and training in antiterrorist operations. The fact that many millions of passengers use the system carries with it the danger of crime, including the possibility of terrorist acts. In view of the movements of an enormous number of people, many of whom are visitors to the capital, the crime situation in the subway

system compels the subway system police unit to operate in a state of constant readiness.

The police road patrol service plays a special role in preventing terrorist acts in the capital. Its officers keep a 24-hour watch at state road inspection checkpoints and inspect the flows of cargo arriving in the capital.

MVD units provide antiterrorism protection to facilities of special importance, those vital to life and welfare, and those presenting a heightened degree of danger (including heating and power stations, dams, and water pumping stations, which have active chemically dangerous substances stored on site). Many of the facilities have installed video cameras that are monitored at guard stations by enterprise security personnel. Special police emergency call systems have been installed at these facilities. Some of the sites are equipped with fire alarm systems linked to centralized alarm centers at local district units of the MVD.

A wide-scale educational campaign has been launched to develop a sense of watchfulness among the population and instill basic habits of proper behavior during bomb threats. Police units are constantly providing the public and passengers with specially prepared reminders on what to do if they find unattended or suspicious objects. Similar training sessions have been organized for subway train operators and drivers from the various passenger transport enterprises. Created for terrorism prevention purposes, the antiterrorism automated search system facilitates the efficient exchange of information on the movements of persons of interest to us and the registration of members of extremist organizations.

The sharp increase in the number of terrorist incidents in 1999 served as a warning signal that strategies and tactics for countering the advance of terrorism were in need of review. Even then, three years ago, it was noted that there had been some unfavorable qualitative changes in the structure of this type of violent crime. In particular, the overall proportion of attempts on the lives or health of people increased, with a complementary decrease in the share of crimes targeting material objects. Crimes became bigger in scope, being characterized by large numbers of human victims, and terrorists became increasingly brutal and brazen. Moreover, terrorist societies and groups received an expanded amount of informational, tactical, and mutual resource support. Political and criminal terrorism coalesced against a backdrop of convergence and cooperation of illegal and legal structures of an extremist nature with nationalist, religious separatist, fundamentalist, and other organizations on the basis of their mutually beneficial interests.

Our prime task is to coordinate the antiterrorist activities of federal executive-branch agencies in their interactions with analogous agencies at the republic, oblast, and local levels and with enterprises, institutions, and organizations with the aim of increasing the efficiency of measures to discover, prevent, and suppress terrorist activities. In cooperation with other law enforcement agencies at the local and federal levels, the MVD is continuing to work actively towards further exposing the terrorist underground.

It should be noted that scientific research on the circumstances in which terrorist acts are carried out, the personalities of terrorists, and so forth, plays a special role in preventing crimes of a terrorist nature. By analyzing acts of terrorism that have taken place, it is possible to arrive at several particular features or, if you will, laws of operation (see Figures 1–5).

The diagrams graphically illustrate the facilities and individuals that should be the focus of top-priority preventive work, and this allows us to define the basic objectives this work should entail.

The well-known events at the theater center on Dubrovka Street have forced us to increase our efforts to rid the capital’s economy of the “ethnic crime business.” In 2002 we uncovered more than 500 enterprises under various forms of ownership that were, according to operational data, involved in

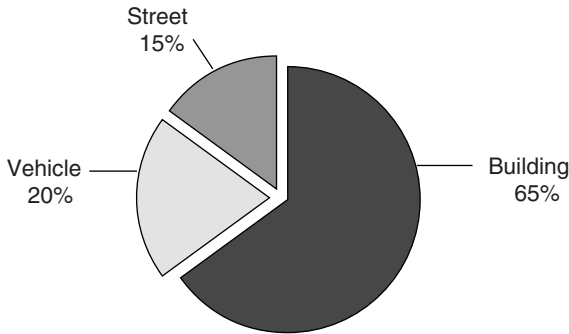


FIGURE 1 Distribution of terrorist acts committed in Russia by location.

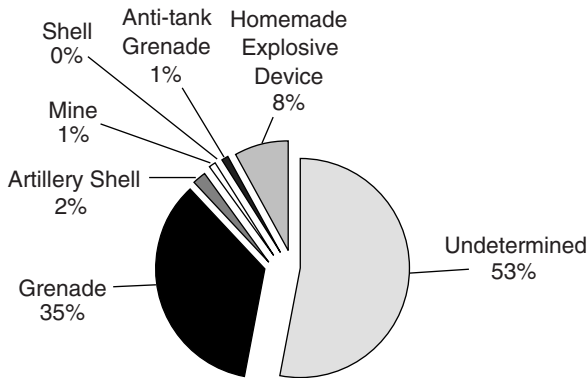


FIGURE 2 Distribution of bombings in Russia by type of explosive device used.

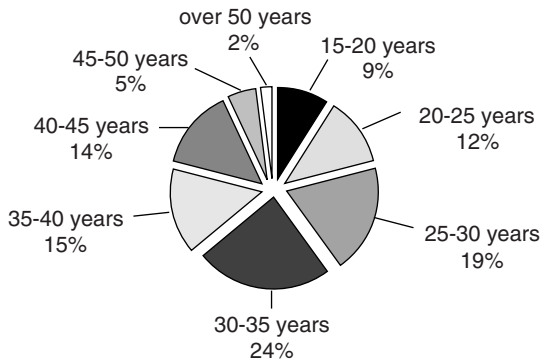


FIGURE 3 Distribution of terrorists by age.

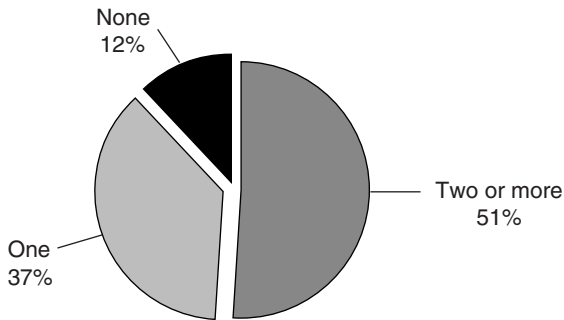


FIGURE 4 Distribution of terrorists by number of previous convictions.

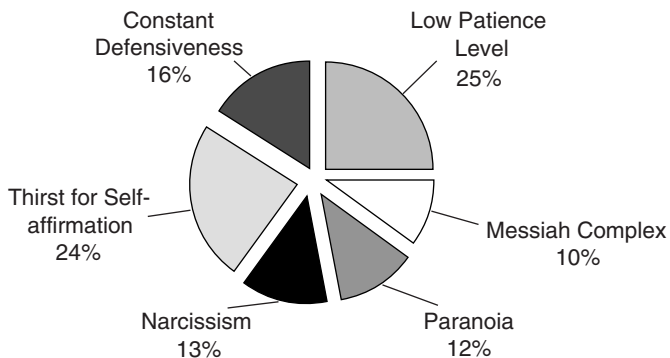


FIGURE 5 Psychological characteristics of terrorists' personalities.

providing financial or other support to criminal groups composed of individuals from the North Caucasus region and the Caucasus republics. Already in 2003 we have discovered more than 200 commercial entities in Moscow that are controlled by Chechen, Dagestani, Azerbaijani, Armenian, and Georgian organized crime groups.

The criminal groups mentioned above have a most negative effect on the operational situation in Moscow. In comparison with similar Slavic groups, these groups are the source of greater social and public danger. Relations within them are founded on familial and clan-based principles. Crimes in which they are involved are, as a rule, well organized, brutal, and unpredictable in nature. Furthermore, while criminal bombings carried out by Azerbaijani or Georgian organized crime groups are primarily a means of eliminating criminal business competitors, the situation with Chechen groups is different. In addition to the criminal component, we frequently see attempts to exert pressure on the political situation, to use terror to obtain changes in the federal government's position on settlement of the Chechen crisis.

There have been certain positive developments, specifically, in uncovering and cutting off flows of weapons, explosives, and narcotics into the capital. For example, on December 24, 2002, while investigating reports of the arrival in Moscow of Chechens aiming to carry out terrorist acts, our personnel in cooperation with colleagues from the FSB arrested two individuals from Chechnya and confiscated two suicide vests with explosives, military grenades, and a remote control device. On January 20, 2003, an ethnic crime group was arrested while bringing a large quantity of narcotics into Moscow. More than 40 kg of heroin was seized.

I would now like to say a few words about our views of what we must accomplish in our efforts to fight terrorism.

- A unified database on extremist groups and their leaders must be created.
- Heavier administrative and criminal penalties should be established for those who participate in street riots and promote extremist means of political struggle.
- The political process should be monitored not only in Moscow but also in the various republics and oblasts that make up the Russian Federation (including small cities where the socioeconomic and ethnopolitical situations are strained).
- Guided by the experience of Israel, Spain, and other countries, a modern antiterrorist infrastructure should be formed, including the secret services, the media, public and religious organizations, the educational system, and the migration service.
- It would be expedient to set harsher punishment for illegally dealing in weapons and explosives and committing crimes involving the use of firearms in order to ensure that judicial proceedings for such criminal cases are appropriate to the danger they present to society.

- In cooperation with the media, an information campaign should be organized to persuade the public to voluntarily surrender illegal weapons, explosives, and ammunition.
- The protection of dangerous facilities should be increased, perimeter barriers around them strengthened, and video monitoring, alarm, and control systems installed at their entrances and exits to facilitate immediate notification of the presence of weapons and explosives.
- A solution must be found to the question of creating centers in large cities to hold migrants who have been found to be in Russia illegally and who have been issued court orders for forcible removal from the Russian Federation. A mechanism for financing their deportations must also be worked out.
- Increased administrative penalties should be put in place for violations of passport and visa regulations in special status locations (republic and oblast capitals, regions where especially dangerous industrial facilities or atomic power plants are located, and so forth).
- All government agencies should increase their efforts to prevent and suppress commercial activities associated with the illegal trade in weapons, drugs, prostitution, and pornography; the illegal reproduction of information on computer disks or tapes; illegal operations involving foreign currency and antiques; and so forth, as all of these activities produce large profits that can be used to finance terrorists and extremists.
- Measures should be taken to identify enterprises and firms involved in organizing the illegal migration of foreign citizens. The activities of organizations and firms inviting foreign citizens from abroad should be monitored, especially if they involve citizens from countries that are militarily, politically, or economically unstable. Action should be taken to prevent the uncontrolled movement throughout the Russian Federation of individuals without identity papers and foreigners who refuse to leave the country when the authorized duration of their visit has expired.
- It would seem appropriate to increase the amount of funds available for rewarding citizens who assist internal affairs agencies in identifying and exposing individuals planning or committing terrorist acts and their accomplices.
- With the aim of controlling cargo shipments and preventing the possibility that weapons, explosives, and explosive devices might be transported to major cities along with agricultural or other products, special terminals equipped with monitoring equipment should be established at the city limits to inspect heavy freight vehicles (refrigerator trucks, semitrailers, and so forth).

The following changes should be made in laws and regulations by various levels of government in the Russian Federation:

- Questions regarding arrest procedures, grounds for arrest, and pre-arraignment detention terms for persons suspected of committing terrorist acts or

serving as accomplices in such crimes should be considered. At present, individuals suspected of committing a crime can be detained for 48 hours, after which they must be formally charged and held or else released. Investigators spend most of this legally permitted period taking care of the various necessary procedural matters, such as preparing the arrest documents, securing a lawyer for the accused, and notifying the prosecutor's office. It is unrealistic to expect that in the remaining time investigators will be able to gather evidence and decide whether the person in custody is guilty or not guilty. Given the degree of danger that terrorism presents to the public, it would seem expedient to temporarily establish special arrest procedures and detention terms for individuals suspected of planning to commit or participate in terrorist acts.

- The MVD, FSB, and Central Bank of Russia should be given expanded powers to institute tighter controls on the activities of individuals and legal entities involved in commercial operations, including those in the wholesale trade business, as well as controls on the use of funds by public organizations and their leaders and activists if operational information indicates that they are involved in financing terrorist activities.

- Internal affairs agencies should be notified when notarized general vehicle licenses are issued.

NOTES

1. Terrorism in modern capitalist society. 1980. (2nd ed.). Moscow: Russian Academy of Sciences Institute of Scientific Information in the Social Sciences. p. 8.

2. See How to defeat terrorism. 2002. Ekspert 41, November 4.

3. On research in this field, see Terrorism—a general threat to security in the twenty-first century: An analytical report. 2001. Moscow: Center for Strategic Development. p. 20.

4. See Terror without borders? An answer will come. 2002. Rossiiskaya Gazeta 206, October 30.

5. The website www.crdf.org provides information on scientific research in the field of victimology.

The Role of the Russian Ministry of Emergency Situations and Executive Branch Agencies of the City of Moscow in Dealing with Emergency Situations Arising from Acts of Terrorism

*Aleksandr M. Yeliseev**

Moscow Main Administration for Civil Defense and Emergency Situations

The problems of ensuring the security of people and territory are a top priority for executive- and legislative-branch agencies of the Russian Federation. The major radiation accident at the Chernobyl Atomic Power Station in 1986 and the destructive Spitak earthquake in 1988 demonstrated the need for creating a Russian system for preventing and eliminating the consequences of emergency situations. The Ministry for Civil Defense, Emergency Situations, and Elimination of the Consequences of Natural Disasters (MChS) became the central component in this system. Territorial subunits of the MChS are among the executive-branch agencies of the various republics and oblasts that make up the Russian Federation, and they act at the local level to implement state policy with regard to protecting people and territory from emergency situations.

Moscow has historically represented the spiritual center of the Russian land. It is Russia's largest industrial center, making a substantial contribution to the country's overall economic indicators. Our city is the country's most important transport hub, on which the operation of the entire Russian transportation system is dependent. It represents the most important concentration of financial and information flows, which has a significant impact on the development of the state as a whole. Moscow is the center of scientific and cultural life, the focal point of a significant part of our national heritage, and a unique world-class historical and architectural center. All of these factors determine the level of the threat to the vital interests of citizens, social groups, and the city as a whole.

*Translated from the Russian by Kelly Robbins.

The following types of threats are most typical: criminal, terrorist, social, political, infrastructural, natural, industrial, environmental, informational, and psychological. These threats are of a complex and interrelated nature, with the majority being transnational in scale. These circumstances are characteristic of almost all the world's major megacities; therefore, they call for a great deal of attention to be devoted by the city leadership to problems of ensuring the security of urban facilities and residents of the capital.

Here, we proceed from the belief that ensuring the security of the population against emergency situations resulting from terrorism, natural and industrial disasters, and other causes is a difficult and complex task, and carrying it out successfully can be done only with the active involvement of all city departments, agencies, and organizations. Therefore, the Moscow City System for Preventing and Eliminating the Consequences of Emergency Situations was created in 1996, functionally linking the city's various district and departmental services units. City policy for ensuring the security of the population and the urban infrastructure is implemented through the Commissions on Emergency Situations, which have been established in each agency and department of the city administration and which are headed by leaders at the corresponding level. This operating principle facilitates management of the actions of city units in preventing emergencies as well as responding to threats and responding to emergencies once they have occurred. It is also helpful in coordinating the actions of the various services and organizing and efficiently carrying out emergency rescue operations.

In connection with the implementation of a special law passed by the city of Moscow, work is under way citywide to implement a comprehensive targeted program for improving the Moscow city system for preventing and eliminating the consequences of emergency situations. The program was developed on the initiative of the Moscow City Government and the MChS and was supported by the deputies of the Moscow City Duma. The basic goals of the program include

- implementing a set of measures aimed at preventing emergency situations, including the establishment of an effective system for monitoring and predicting accidents, catastrophes, and natural disasters
- modernizing the management and communications system through the widespread use of the latest information technologies
- improving the speed and efficiency of emergency response by creating a highly mobile and technically well equipped rescue service and by developing aviation technologies for use in emergency rescue operations
- improving the citywide system for educating the population on the appropriate actions to be taken during emergency situations

However, in recent years terrorism has been one of the main threats to public security. It presents a special danger to major cities and political, economic, and cultural centers. Terrorist acts are taking on ever-increasing scale and

becoming more and more diverse both in form and in the goals for which they are carried out.

Since 1998, Moscow has been subjected to terrorist attacks on more than one occasion. We remember the bombings of apartment buildings on Guryanov Street and Kashirskoe Shosse, the shopping mall at Manezh Square, the underground passageway at the Pushkinskaya metro station, and the seizure of hostages during the performance of the musical *Nord-Ost*, in which more than 3,000 people were victims, of whom about 600 were killed.

These events have shown that terrorist acts are ever more frequently moving from the realm of potential threats to that of real emergency situations. In our view it is the world community's failure to respond appropriately to the terrorist acts committed in Moscow in the fall of 1999 that led to the tragic events of September 11, 2001, in the United States. Those events demonstrated once again that terrorism has no nationality but rather is international in nature, and not a single state is secure against it.

Expert assessments highlight the broad scope of this phenomenon, and many believe that at present in the various countries of the world there are about 100 major terrorist organizations, which maintain contacts among themselves. Therefore, the problem goes beyond the bounds of individual states. Furthermore, in recent years terrorism has acquired the capability of using the achievements of science and technology to further its criminal aims.

We have great understanding for the position of the New York City authorities, as we ourselves were on the scene only minutes after the bombings of the Moscow apartment buildings in 1999. Under the leadership of Moscow Mayor Yury M. Luzhkov and Russian Emergency Situations Minister Sergei K. Shoigu, we organized efforts to deal with the consequences of these explosions. We provided detailed reports on these incidents to the European community at an international conference in Vienna in 2000.

Antiterrorism activities in Moscow are conducted at all levels of the city government. This work is coordinated by an antiterrorism commission operating under the leadership of the city's mayor, and includes the following activities:

- improving laws related to the struggle against terrorism
- increasing the effectiveness of preventive measures
- ensuring the secure operations of industrial facilities and sites where large numbers of people gather

I would like to say that we have done a certain amount of work to ensure the security of residents and of the capital in general, primarily with regard to the creation of laws and regulations addressing these matters.

The city has recently enacted a Law on Protecting the Population and Territory of the City of Moscow from Emergency Situations of Natural and Industrial Origin. A strategy for the security of Moscow has also been adopted, outlining in

systematic form the views of the city's leadership on ensuring the safety of its residents. In the process of developing this strategy, the programs Moscow Radiation Security and Moscow Chemical Security were also created and adopted to deal with matters related to protecting potentially dangerous facilities against terrorism. In the past few years, Moscow has passed more than 100 regulations governing matters related to the city's security, and we are prepared to acquaint representatives of the international community with them.

Executive-branch agencies are devoting special attention to monitoring and controlling the activities of all officials involved in implementing preventive measures against emergency situations. In 2002 alone, the State Inspectorate for Protecting the Population and Territory from Emergency Situations conducted checks at more than 10,000 enterprises, organizations, and institutions. Those guilty of violating urban security regulations face administrative penalties and are prosecuted through the civilian court system.

City policy regarding new construction is pursued rather effectively. Moscow has established a system of measures that prohibits the construction or reconstruction of any industrial buildings, housing, or other public facilities that do not include design features intended to prevent possible emergency situations, including potential terrorist acts.

The city has created the Center for Monitoring and Forecasting Emergency Situations, for which the main objectives are the prevention and early detection of emergencies. The components of this system include stationary and mobile Lidar units, which use laser, infrared, and visual observation methods to detect fires and atmospheric emissions of harmful substances.

In accounting for the large amounts of special cargo (gasoline, reagents for refrigeration systems, and so forth) that pass through Moscow and other world cities, cargo that also represents a potential threat of the commission of terrorist acts, we have tightened controls on the transport of such materials by road and rail within the city limits. The city's law enforcement agencies are paying special attention to the safety of capital residents in locations where large numbers of people gather, such as markets, fairs, and the sites of large cultural events and sports competitions.

The quality of efforts to prevent and eliminate the consequences of emergency situations depends primarily on the level of preparedness of the leadership, specialists, and city residents. This matter is being addressed by providing training to almost all categories of city residents at special educational institutions, enterprises, and places of residence. For example, in 2002, about 30,000 people received special training at educational centers and more than 2 million blue- and white-collar personnel received training at their worksites.

Training games represent the most effective form of preparation for individuals in positions of leadership. Such games allow participants to practice dealing with matters such as procedures for notification and assembly of senior officials, technologies for application in emergency rescue operations and oth-

er urgent activities, organization of assistance to city service providers in eliminating the consequences of emergency situations, comprehensive provision of aid and services to the affected population, and a number of other citywide undertakings.

Earlier this year, a special tactical training exercise was conducted at a Moscow subway station to focus on coordinating the activities of city services in eliminating the consequences of a possible terrorist act involving the use of dangerous chemical substances. During the training exercise, a number of practical measures were developed with the aim of improving the efficiency of emergency rescue efforts under such conditions, and these measures have now been submitted to the Moscow City Government for review.

Efforts to train young people occupy an important place in our work. Last year, in cooperation with the Moscow Educational Committee, we began training students from the capital's higher educational institutions to serve as reserve rescue personnel. A class entitled "Principles of Everyday Safety" has also been introduced for students in all grades in elementary and secondary schools. The number of participants in "Safety School" competitions is constantly on the rise. Each year, more and more secondary school students participate in "Young Rescuer" summer camps.

Regarding measures to prevent emergencies, we must not forget that the city must also be prepared to eliminate their consequences. The main element of this system is the Center for Crisis Situation Management, which is designed to gather and process information about emergency situations, inform the population, and make well-founded decisions on how to handle such situations.

At present, plans call for the creation of a Unified Monitoring and Dispatch Center for the city of Moscow on the basis of the facilities of the Moscow City Crisis Situation Management Center and the Force Management Center of the State Fire Service Administration of MChS. This new center, which would be reachable by dialing 01, would facilitate the efficient collection and processing of emergency reports, analyze an enormous amount of information under extremely time-critical conditions, and coordinate the actions of all dispatch services included in the city's unified dispatch system.

The current combined daily volume for the two centers mentioned above is approximately 6,000 calls. After the switch to the single telephone number 01, it is predicted that the number of calls alone will rise to 18,000 per day. This will require a large set of organizational and technical changes to be made, taking into account foreign experience in operating rescue services using single telephone numbers such as 112 and 911.

Creating, training, and developing forces for eliminating the consequences of emergency situations is of enormous significance in the functioning of the system. To this end, the Moscow City Search and Rescue Service has been created in the capital. Also operating in cooperation with us in the city are various MChS rescue units and a number of commercial entities. If a major emer-

gency occurs, plans call for augmenting the rescue service by calling in specialists and equipment from other city organizations.

Since the city search and rescue service was established, rescuers have carried out about 60,000 rescue operations and have saved more than 25,000 people. In 2002 alone, Moscow firefighters handled about 7,000 fires. The timely and skillful actions of personnel from the city's medical service have saved the lives of thousands of Muscovites involved in emergency situations and accidents.

Unfortunately, Muscovites have been forced to confront inhuman acts of terrorism in practice. We profoundly share the pain and suffering of other nations affected by emergency situations of any kind. Therefore, the government of Moscow is devoting a great deal of attention to humanitarian operations, including those of international scope. We are providing humanitarian aid to the suffering population in various regions of Russia and in other countries, including Kosovo, Afghanistan, Korea, Bolivia, the Balkans, Germany, the Czech Republic, and others.

Overall, we may conclude that the government of Moscow has a great focus on international cooperation in combating terrorism and crime and eliminating the consequences of terrorist acts and natural and industrial disasters. In recent years, stable contacts have been established among counterpart police and emergency services agencies at the municipal level as part of the comprehensive cooperation between Moscow and foreign cities, including those in Europe. Close cooperation is under way with the cities of Vienna, Berlin, Madrid, Dublin, Helsinki, and others in the form of information sharing, exchanges and training of specialists, and joint training exercises.

In May 2002, on the initiative of Moscow Mayor Yury M. Luzhkov, a meeting of police officials from European countries was convened to promote better coordination in the struggle against terrorism. Moreover, an international meeting on matters of security in major cities is to be held in Moscow in June 2003.

In conclusion, I would like to say that the system that has been created in Moscow for preventing and eliminating the consequences of emergency situations stands ready to cooperate closely in the twenty-first century with any who treasure the ideals of humanism and defense of the most important human right, the right to life.

Papers from
*Countering Urban Terrorism in Russia and
the United States:
Proceedings of a Workshop (2006)*

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.

Radiochemical 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

- 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)

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.

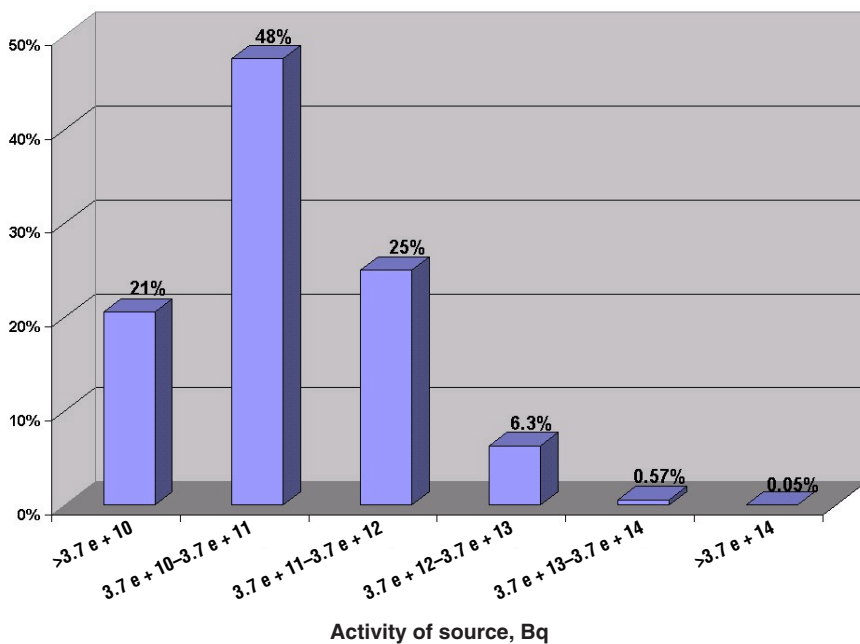
and imperfections in the system for accounting, licensing, regulating, and control, which make it difficult to bar all paths of illegal movements of ionizing radiation sources, especially in nonnuclear industries.

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

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

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

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

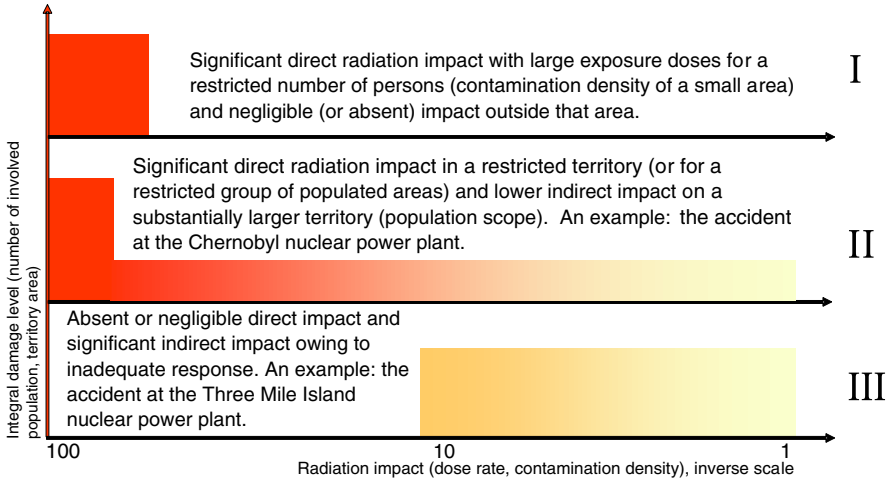
- the current state of physical protection systems
- security procedures at the facility where ionizing radiation sources are present
- economic and financial stability of the facility
- location of the facility in terms of ease of unauthorized access

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. Regrettably such assessments do not fully take into account the interrelation between health consequences, socioeconomic consequences, and the design of the dispersion device.

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



The integral damage in the tail might substantially exceed that in the core (if any).

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.

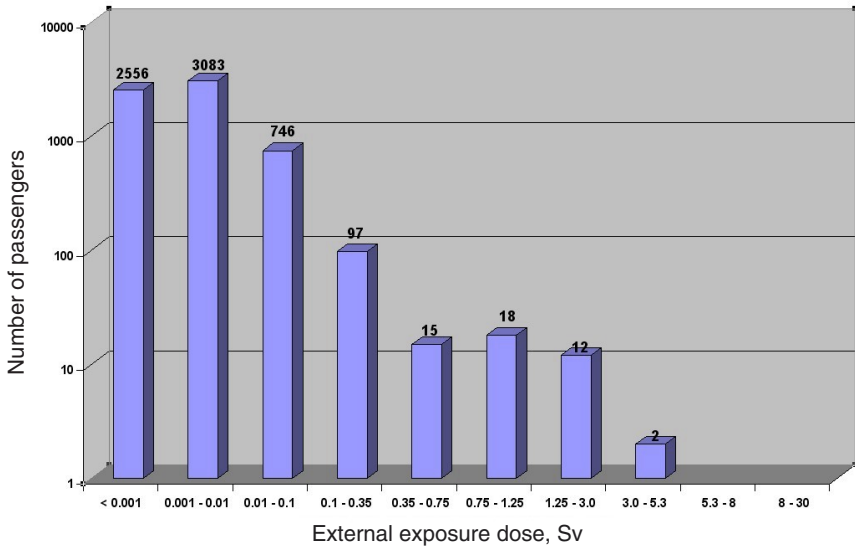


FIGURE 3 Distribution of the subway car passengers by whole-body external exposure doses.

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

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 km² of the city being contaminated to higher than 1 Ci/km². 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/km² 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-

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

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-

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

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 socio-psychological 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-

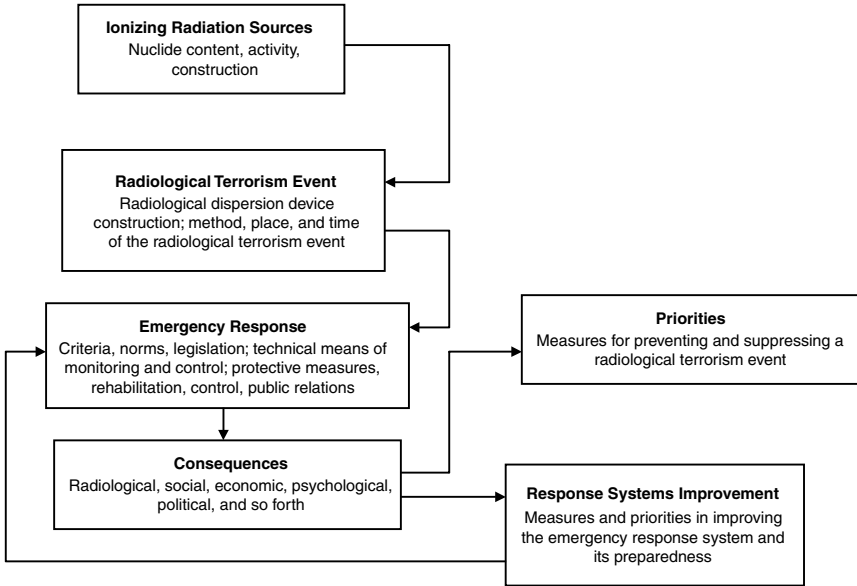


FIGURE 4 Factors determining radiological terrorism consequences and their interrelation.

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

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-

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 km²), the average survey zone of such a station is about 7 km², 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 μ R/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-

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)

Source and its activity	Distance, m			
	One rotation of collimator (6 s)		10 rotations of collimator (1 min)	
	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 ^3He 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

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.

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.

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 model¹ was used for estimating fire endurance time.

The main system of equations consisted of

- mass conservation equation
- energy conservation equation

¹Koshmarov, 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.

- 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 $50 \times 50 \times 10$ 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

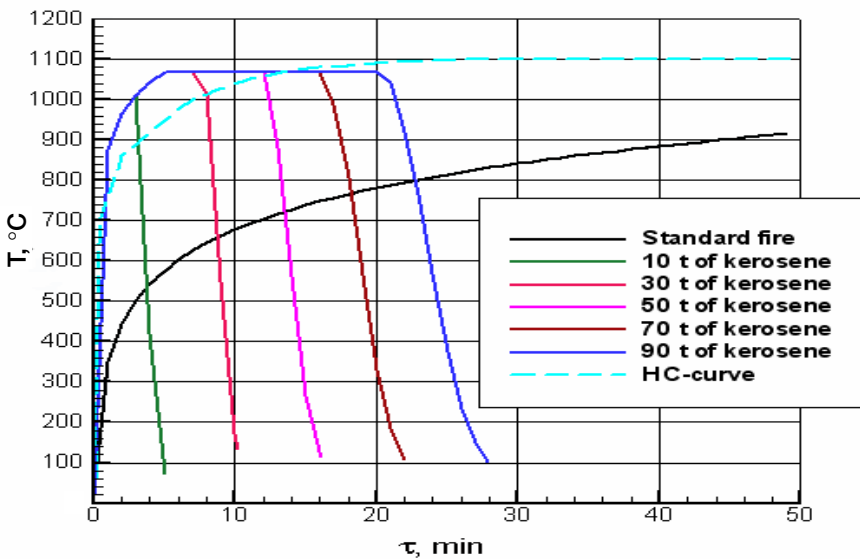


FIGURE 1 Dynamics of average temperature in the enclosure with various quantities of combustible in the form of spilled kerosene.

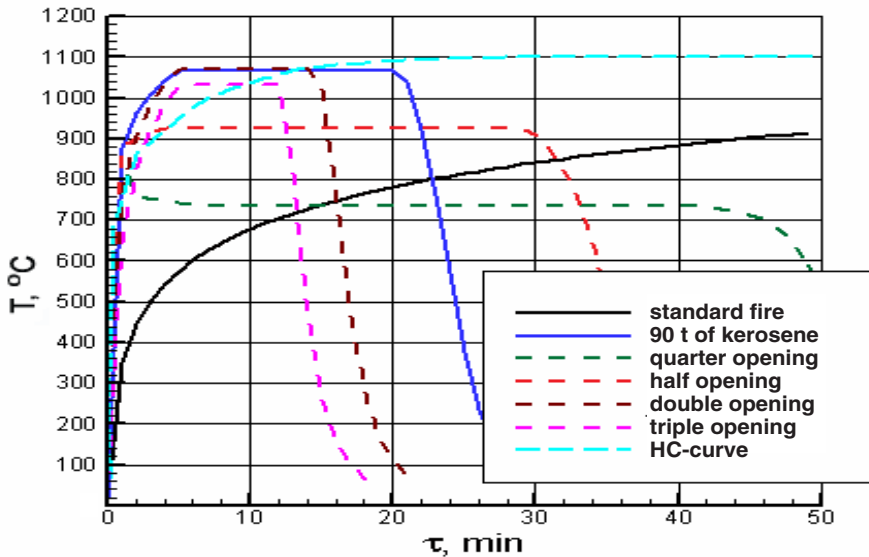


FIGURE 2 Dynamics of average temperature in the enclosure during combustion of 90 metric tons of kerosene with different sizes of opening areas.

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-

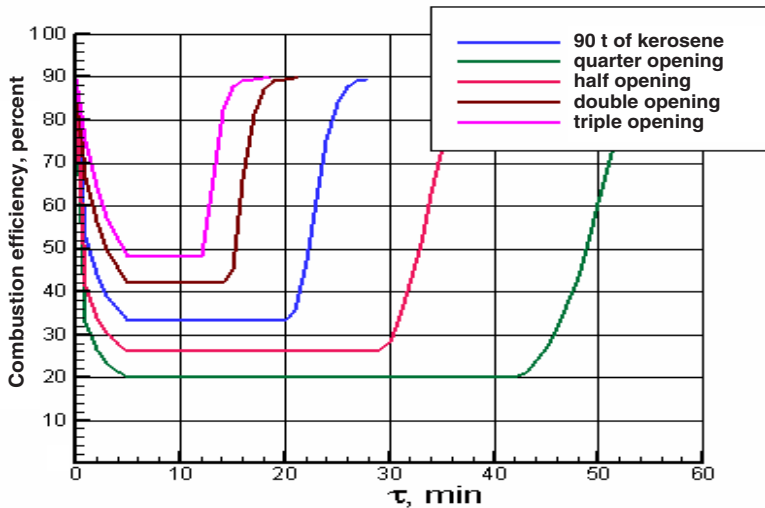


FIGURE 3 Variation of combustion efficiency during combustion of 90 metric tons of kerosene with different sizes of opening areas.

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/m² (in

²Central 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.

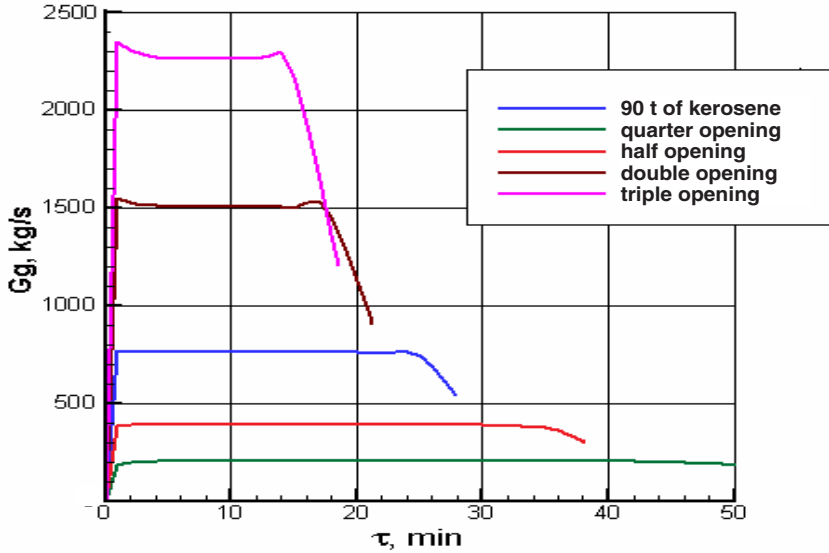


FIGURE 4 Dynamics of mass flow of gas emissions (G_g) during combustion of 90 metric tons of kerosene with different sizes of opening areas.

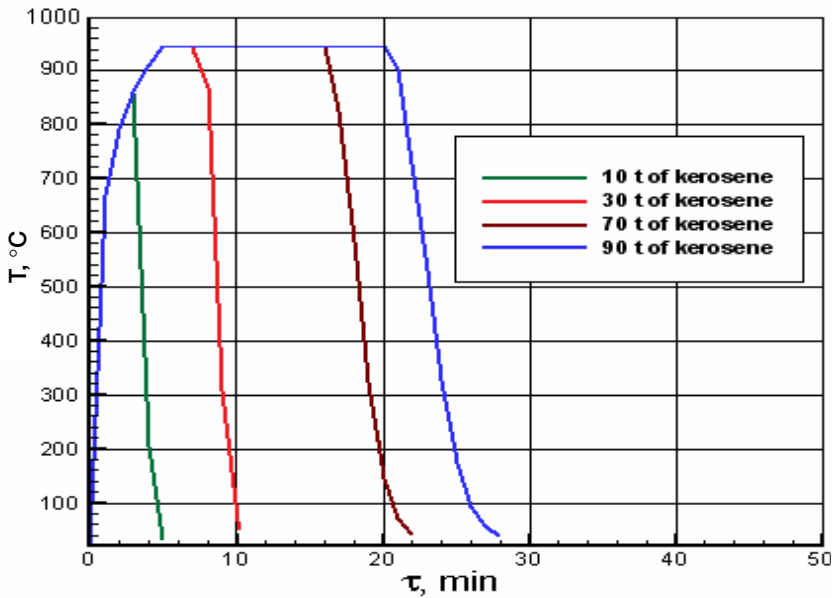


FIGURE 5 Dynamics of the temperature of the enclosure walls with different quantities of combustible spilled kerosene.

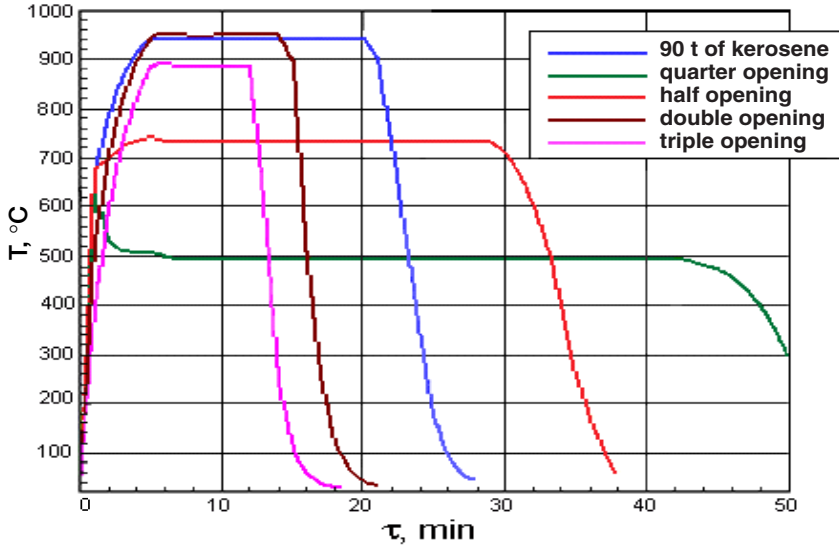


FIGURE 6 Dynamics of the temperature of the enclosure walls during combustion of 90 metric tons of kerosene with different sizes of opening areas.

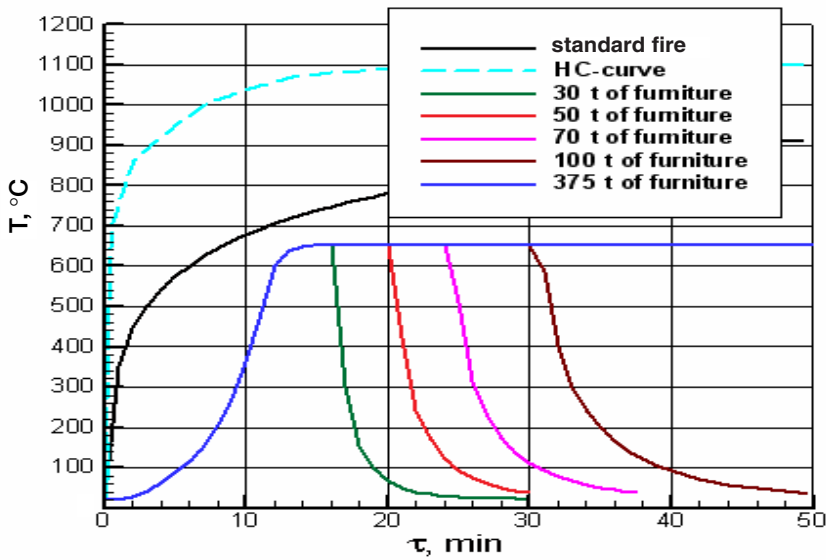


FIGURE 7 Dynamics of average temperature in the enclosure with various quantities of furniture.

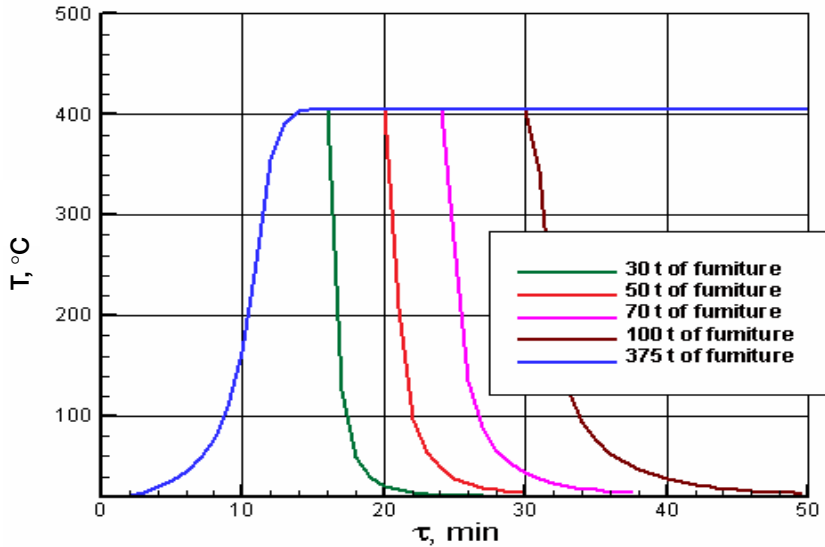


FIGURE 8 Dynamics of average temperature of the enclosure walls with various quantities of furniture.

wood). Thus, given that the floor area of that enclosure (damage zone) equals 2,500 m² 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.

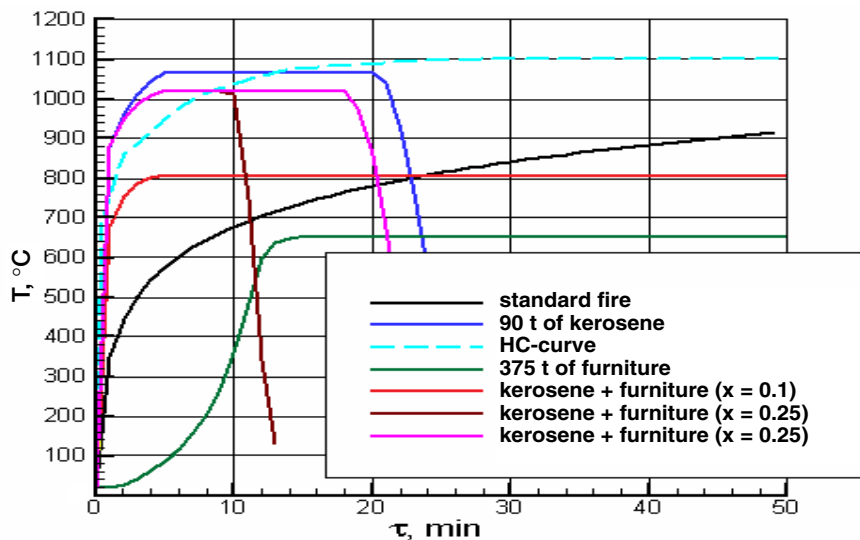


FIGURE 9 Dynamics of average temperature in the enclosure with various quantities of kerosene in the combustible load.

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 $500\text{ }^\circ\text{C}$ ($\pm 50\text{ }^\circ\text{C}$; 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

³Hamburger, 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.

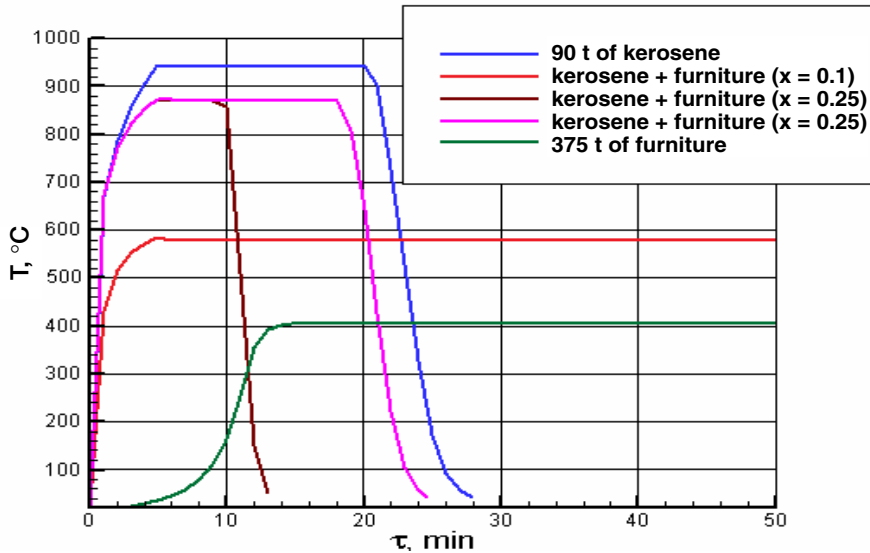


FIGURE 10 Dynamics of the temperature of the enclosure walls with various quantities of kerosene in the combustible load.

and bearing columns. Ten floor panels with dimensions $5.1 \times 1.2 \times 0.22$ 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 $P_{\text{panel}} = 1,067 \text{ kg/m}^2$ and the column loading was $P_{\text{column}} = 120$ 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 $\alpha_c = 0.03$, fire endurance time falls by 6 percent, and for $\alpha_c = 0.14$, 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.

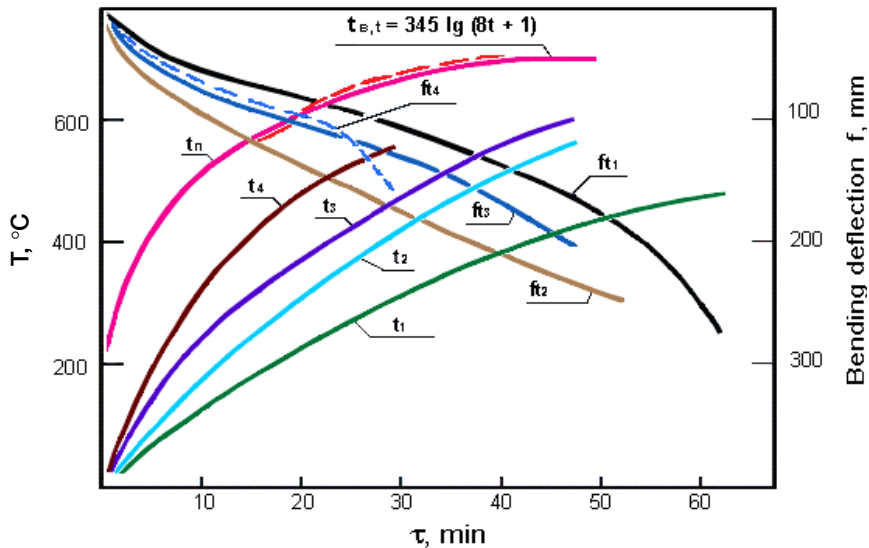


FIGURE 11 Temperature change and maximal bending deflection during fire resistance testing of hollow-core slabs.

Note: $t_{B,t}$ —standard temperature fire regime, °C; t_n —actual temperature of the fire chamber, °C; $t_{1,2,3,4}$ —average values of the reinforcement heating, °C; $ft_{1,2,3,4}$ —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.

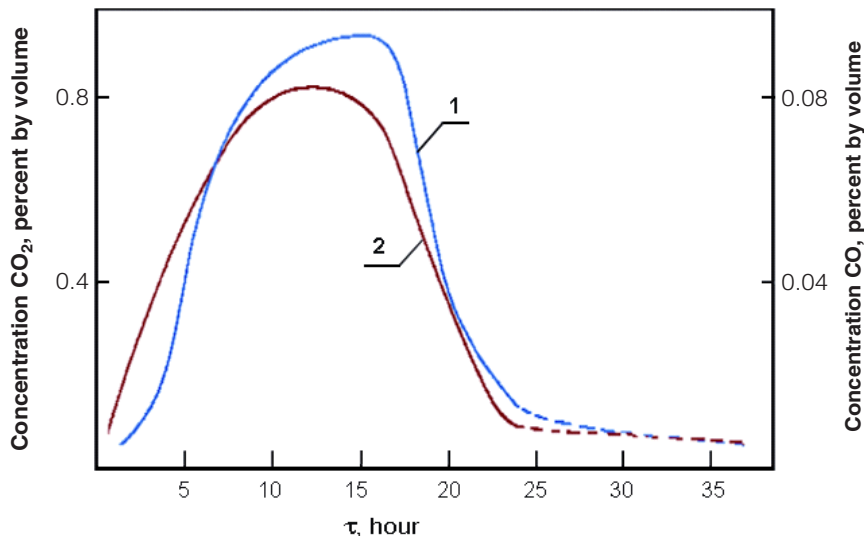


FIGURE 12 Average CO and CO₂ concentrations at fires in the ruins of a one-story brick building of the second fire resistance class.

Note: 1—CO concentration; 2—CO₂ concentration.

Figure 12 shows an average of experimental data illustrating the dynamics of fire hazard factors (CO and CO₂ 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,

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

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 .

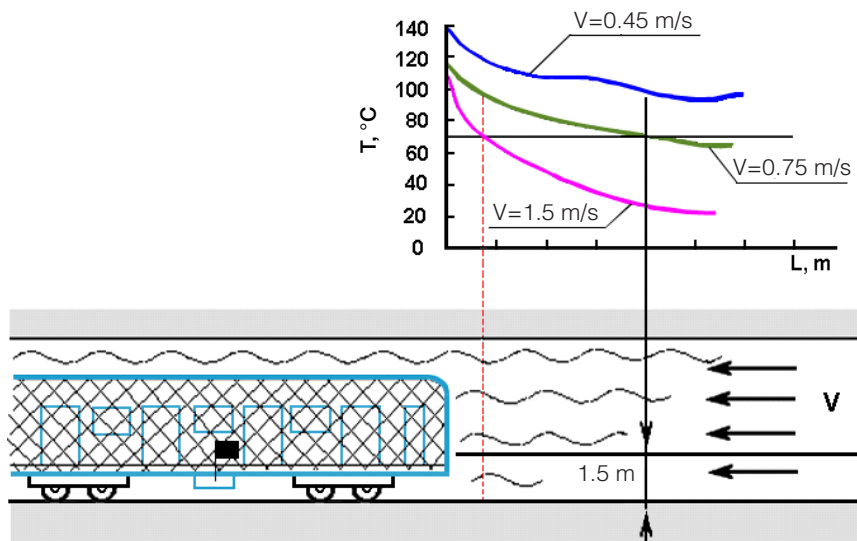


FIGURE 13 Temperature in the vicinity of the burning train car.

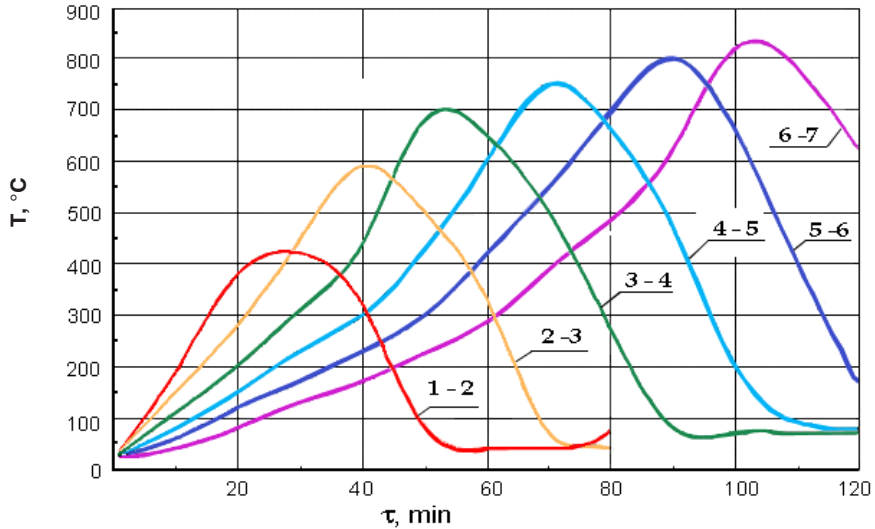


FIGURE 14 Temperature regime of a burning subway train.

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

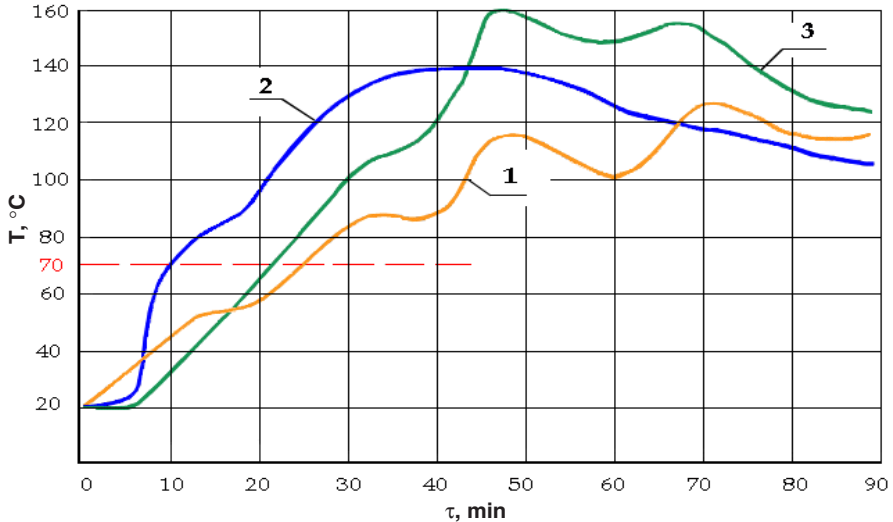


FIGURE 15 Temperature of the subway station during rolling stock fire.

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

⁴Galea, 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.

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.

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 m², 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

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.

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-

ists. In fact, it was the first major terrorist act carried out by members of the so-called Riyadus Salihii scouting and sabotage battalion created by Shamil Basaev (in Arabic, “Riyadh as-Salihii” 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

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

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

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 counter-terrorist 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.

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

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 Aslakhonov 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

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.

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 indicators 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

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

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.

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

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

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.

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

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.

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

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

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

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.

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

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.

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.

¹Knowledge 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.

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

²Translator'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.

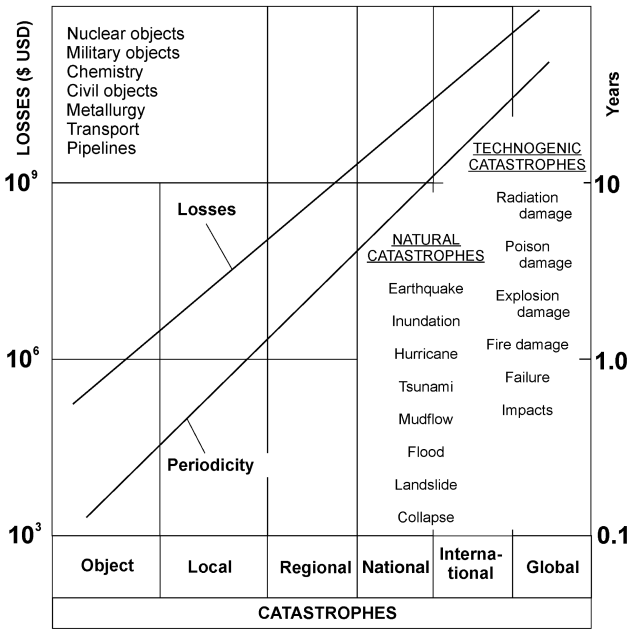


FIGURE 1 Losses and periodicity of natural and technogenic catastrophes.

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-

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

³Knowledge 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.

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

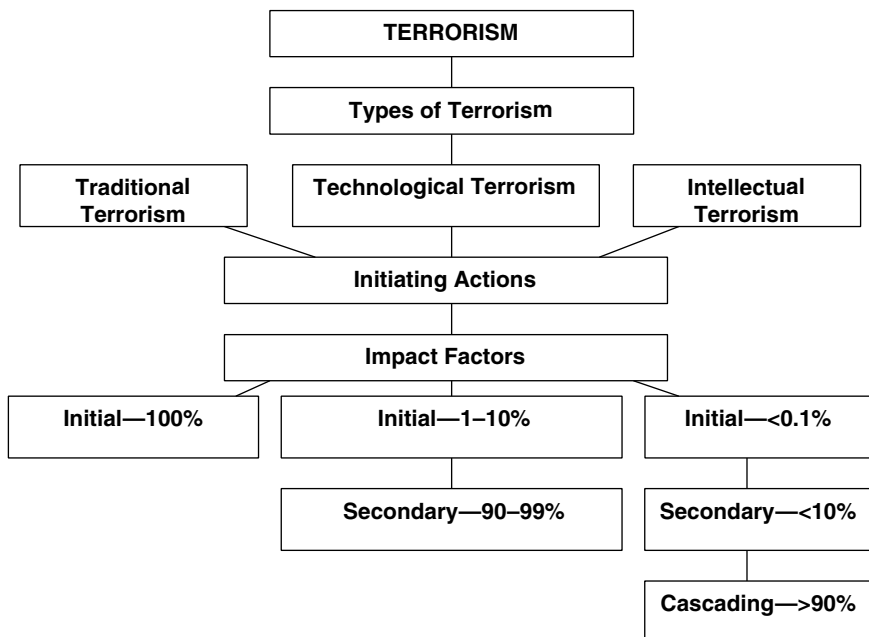


FIGURE 2 Types of terrorism and impact factors.

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, crisis 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

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 $\nu(t)$. 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:

$$R = F_R\{R_E, R_W, R_I\} = F_R\{(P_E, U_E), (P_W, U_W), (P_I, U_I)\} \quad (\text{Formula 2})$$

The fundamental special feature of terrorism risks according to Figure 3 is that a common random process $\nu(t)$ 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-

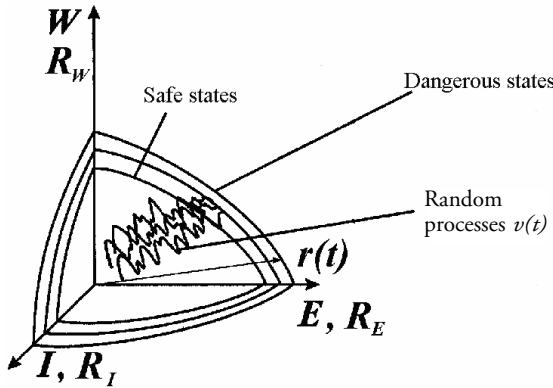


FIGURE 3 Areas of dangerous and safe states.

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:

$$R_{TR} \geq R, \quad r(t) < v(t), \quad t_{TR} < t_0 \tag{Formula 3}$$

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).

$$R_s = \sum R_i, \quad R_i = \sum R_d, \quad R_d = \sum R_e \tag{Formula 4}$$

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:

$$P_S = F_{PS} \{P_N, P_T, P_O\} \quad (\text{Formula 5})$$

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_O 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_O .

$$P_{OTR} = F_P \{(P_{NTR}), (P_{TTR})\} \quad (\text{Formula 9})$$

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.

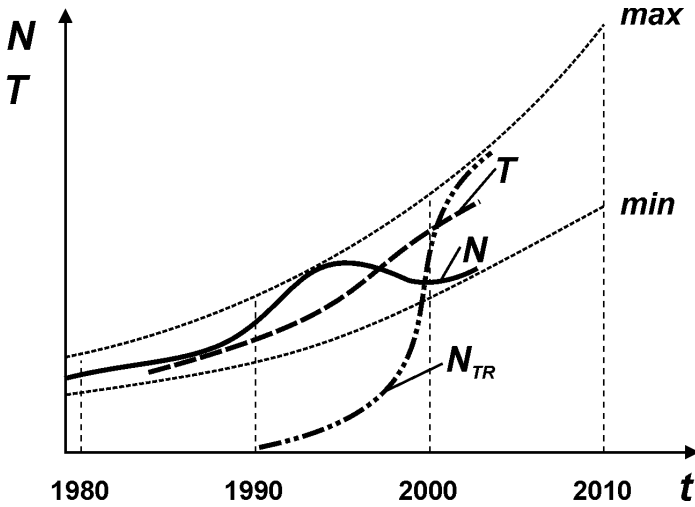


FIGURE 4 Change over time in the number N and severity T of catastrophes.

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]:

$$R_s = P_s U_s \leq (1/n_s) \cdot [R_s] = (1/n_s) \cdot [P_s] \cdot [U_s] = F_z(m_z Z) \quad (\text{Formula 14})$$

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 ($1 \leq m_z \leq 10$).

Security according to the risk criteria R_s may be considered assured if the inequality $n_s \geq 1$ 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 ($\Delta t = 1$ 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:

- 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

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

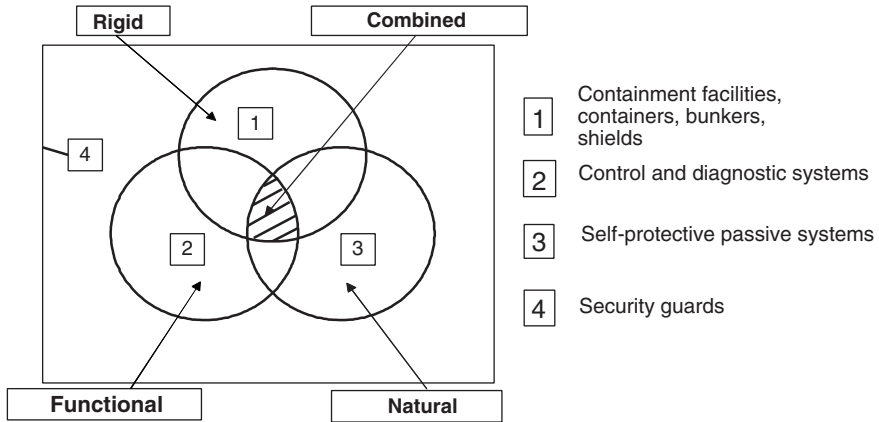


FIGURE 5 Types and systems of protection against accidents and catastrophes.

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

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. Malinetsky. 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 Contemporary Methods of Preventing and Countering Terrorist Activity. P. 244 in *High-Impact Terrorism: Proceedings of a Russian-American Workshop*. Washington, D.C.: National Academy Press.

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.

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.

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.

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.

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.

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:

- 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

- 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
- 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

- 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.

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

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.

- 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.

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

¹For 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.

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.

²According 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.

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

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

³A 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).

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.

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.

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.

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:

- 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 counter-terrorist 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
 - assurance 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-

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

- 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

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

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.

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:

- 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,

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

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

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.

Papers from
*Countering Terrorism—Biological Agents,
Transportation Networks, and Energy
Systems:*
*Summary of a U.S.-Russian Workshop
(2009)*

Electromagnetic Terrorism: Threat to the Security of the State Infrastructure*

*Vladimir Ye. Fortov, Russian Academy of Sciences (RAS)
Moscow High Temperature Institute, and
Yury V. Parfyonov, RAS Institute of High Energy Densities*

A real danger has arisen in recent years, namely, the possible appearance of a new variety of terrorist acts—so-called electromagnetic terrorism. This term refers to the intentional use of powerful electromagnetic pulse emitting devices or high-voltage pulse generators with the aim of disrupting the normal operations of a country's technical systems. Such systems include, for example, aircraft takeoff and landing control instrumentation; telecommunications systems; electronic devices used in managing nuclear power plant operations; systems for electricity generation, transmission, and transformation; equipment used in protecting environmentally hazardous facilities; and so forth.

The world has seen the creation of many powerful electromagnetic pulse generators capable of knocking modern electronic systems out of commission. We shall cite an example of one such piece of equipment that has been created in the laboratory. It consists of a semiconductor-based high-voltage short-pulse generator and an amplifying emitting antenna. Electromagnetic pulses with amplitude on the order of 5 kilovolts per meter and length of about 0.2 nanosecond are formed at a distance of about 10 meters from the emitter. The feature that

* Translated from the Russian by Kelly Robbins.

makes this unit unique is its compactness. We direct your attention to the maximum size of the generator, which is only about 30 centimeters. Further reductions in the size of the generator are possible, and a flat antenna may also be used.

Existing small high-voltage pulse generators make it possible to inject into data transmission chains or even into buildings' electricity supply and grounding networks pulses that are harmful to the equipment located in such buildings. They form short pulses with amplitude of 80 kilovolts, periodically repeating at a frequency of 1,000 gigahertz. Such a generator could be manufactured with a volume on the order of 500-800 cubic centimeters.

There are two possible scenarios for how acts of electromagnetic terrorism could be carried out using powerful electromagnetic sources. Option 1 would be by aiming a powerful electromagnetic field at a facility, and option 2 would be by injecting high-voltage pulses into the data transmission lines and into the electricity supply and grounding network in buildings. To assess the degree of danger presented by these scenarios, a large number of facilities were studied to determine their resistance to the impact of powerful super-broadband electromagnetic radiation and high-voltage pulse disruptions. The results of the experiments show that the intentional use of powerful pulse disruptions could lead to dangerous wide-scale consequences, such as communications breakdowns, power failures, alarm systems blockages, and so forth.

At the same time, it must be said that the designers of the most critical facilities recognize this danger and apply all possible measures to protect electronic systems from various types of electromagnetic disruptions. However, there is an enormous quantity of civilian-use electronic equipment for which there are no requirements for protection against powerful electromagnetic disruptions. Of course, if a few individual pieces of such equipment crash, there will be no serious consequences. Meanwhile, if such equipment fails on a massive scale, chaos will ensue. Therefore, systematic studies have been initiated regarding the stability of civilian-use technical systems against intentionally directed electromagnetic impacts. As an example, presented below are the results of tests on an electronic electricity-use meter and electric power line isolators.

The typical electricity meter is a complex device that includes a special integrated system, a microcontroller, power-independent memory, flow sensors, a pulse power source, an optical port, a liquid crystal indicator, a quartz generator, and a light diode. Experiments have indicated that if the meter is irradiated from a distance of 10 meters, operational failures occur. Furthermore, the personnel responsible for the electricity-use monitoring and accounting system are, as a rule, not capable of establishing the causes of the equipment failure in a timely manner or taking effective measures to eliminate them. Thus, the vulnerability of electronic electricity meters has been established experimentally. The tests have also demonstrated the fundamental possibility of intentionally disrupting their operating capacity for criminal purposes, for example, for unauthorized selection

of a favorable electricity rate, and so forth. It is significant that these actions could be taken remotely and without anyone's notice.

As previously noted, electric power line isolators were among the items tested. A transformer substation would undoubtedly be a more interesting test subject; however, it is too expensive. Therefore, high-voltage isolators were selected as a focus of the experiments instead. The results of these tests are extremely interesting. It is generally believed that technical systems that include semiconductor devices are the most sensitive to the effects of pulse disruptions. As for high-voltage equipment, it is deliberately deemed resistant to such disruptions. This conclusion is based on the results of standard tests on high-voltage equipment for the impact of such disruptions in the absence of operating current. However, in actual conditions, the equipment will be simultaneously affected by both the disruptions and the operating current. Therefore, researchers concluded that special studies were needed. An experimental setup was developed for this purpose. The unit reproduces the joint action of short pulses of up to 400 kilovolts and operating electric current of up to 30 kilovolts. Electric power line isolators were tested using this setup.

Experiments on the isolators showed that with the simultaneous effects of high-voltage pulse disruptions and operating current, degradation of the isolators' electric parameters was observed along with their mechanical destruction. Such effects may lead to catastrophic phenomena in power systems similar to the widespread failure in the Mosenergo system in the summer of 2005 or the fire that broke out in the cable collector in Moscow's Central District in July 2006.

Thus, the experimental data indicate that compact super-broadband electromagnetic pulse emitters and high-voltage pulse generators could easily be used in dishonest competitive struggles, in unauthorized and unnoticed lowering of rates paid for electricity, in the organization of power system failures, and so forth. It would seem reasonable not to wait for these potential threats to be realized but instead to take timely measures to prevent them. Such measures would include evaluating the vulnerability of the most important infrastructure elements. It is also necessary to develop effective measures to protect infrastructure elements from electromagnetic terrorism. Perhaps a review and clarification will also be needed regarding rules for grounding devices and means of laying data transmissions lines, power cables, and so forth.

Because terrorism has become international in recent years and is evoking serious concern in all industrially developed countries, it would be expedient to take measures to promote international cooperation on this issue. It seems necessary to organize a joint experiment to assess the real danger of electromagnetic terrorism and develop means of protection. In addition, international and Russian standards must be developed with the aim of providing better protection for the civilian infrastructure against intentionally directed electromagnetic impacts.

Use of Predictive Modeling Packages for Effective Emergency Management*

*Nikolai Petrovich Kopylov and Irek Ravilevich Khasanov,
All-Russian Scientific Research Institute for Fire Protection (VNIPO) of the
Russian Ministry for Civil Defense Affairs, Emergencies, and Elimination of
Consequences of Natural Disasters (EMERCOM)*

INTRODUCTION

About 1,000 major disasters and catastrophes occur each year in Russia. As a result of industrial and other technogenic¹ accidents alone, more than 200,000 people annually are injured or mutilated and more than 50,000 are killed (including traffic accidents). The economic losses from technogenic and natural disasters total 6 to 7 percent of the country's gross domestic product.²

An analysis of terrorist acts indicates that providing antiterrorism protection for facilities at risk of fire or explosion is the most urgent and important aspect of guarding against terrorism of a technogenic nature. Given these conditions, the effectiveness of management decisions made in eliminating the consequences of acts of technogenic terrorism largely depends on informational and analytical support and predictions of how fires and emergencies might develop.

The primary goal of the integrated state system for predicting and eliminating the consequences of extreme situations is to integrate the efforts of executive branch agencies at both the federal and the Russian Federation subject levels. The main objectives of activities under the state system are as follows:

*Translated from the Russian by Kelly Robbins.

- Monitoring and predicting extreme situations
- Training specialists in emergency prediction and response
- Educating the public on actions to be taken in emergencies
- Developing preventive measures to reduce the risks and lessen the consequences of emergencies
- Improving the management of emergency prediction and response measures

Effectively accomplishing these objectives is impossible without utilizing new information and telecommunications technologies.³

The National Crisis Management Center (NCMC) has been created in Russia to unite the information resources and functional capabilities of local subsystems of the integrated state system with the aim of improving the quality and timeliness of management decisions on predicting and eliminating the consequences of emergencies. The NCMC is a geographically distributed information management complex with peripheral elements that make it possible to manage the forces, means, and resources of the integrated state system and civil defense entities during crises and emergencies.⁴

SITUATION MANAGEMENT CENTERS

The rapid development of information technologies has led to the appearance of massive amounts of informational, communications, audio, and video data that must be recognized, structured, and analyzed in order to make competent management decisions. Meanwhile, although the rates of information technology development have increased, the amount of time allotted for making management decisions is being reduced, especially for decisions made in crisis situations.

The strategy for creating and developing national security support systems by states attests to the fact that information and management centers created at the national and regional levels and in major cities represent the universal foundation for the crisis management system. Informational support for such centers is provided by services such as 911, 112, and 01, as well as by scientific and academic centers.⁵

Intensive efforts are under way to apply modern concepts for the creation of crisis management centers involving high-technology equipment for communications and information exchange, depiction, and processing, which helps in efficiently preparing and making well-founded management decisions. Situation centers have been created in Moscow and regional centers in the various territorial agencies of EMERCOM. These centers are complexes of programmatic and technical resources housed in special facilities where emergency response officials may assemble if an emergency arises. The situation centers regularly conduct training exercises, some of which involve members of the commission on extreme situations.

The activities of a situation center represent the most expedient means of implementing the decision support system based on technologies for numerically simulating and creating visual representations of situations and object behavior. They are the top level in the system for managing the organization, the industry, the region, and the country.

The situation center is an information analysis system that makes it possible to assess the real status of the object or event being managed, detect trends as external and internal changes develop, and analyze (simulate) possible consequences of management actions.⁶ From the most general standpoint, the situation center (room or hall) could be called a facility from which ongoing emergencies are observed or possible situations are analyzed. However, such an interpretation fails to take many factors into account. The modern understanding of a situation center focuses on the entirety of programmatic and technical resources, scientific and mathematical methods, and engineering solutions for automating processes for situational depiction, numerical simulation, analysis, and management.⁷ All of these means and methods make possible the following:

- Providing information on matters where operational decisions are required
- Visually depicting management situations to reveal cause-effect relationships for events being analyzed
- Numerically simulating and conducting situational analyses
- Effecting operational control over efforts being carried out by structural subunits
- Verifying execution of decisions made

The situation centers include various types of analytical support capabilities (programmatic, technical, linguistic, psychological, and so forth). The situation center has four basic levels: (1) scientific-mathematical, (2) engineering, (3) programmatic, and (4) technical.

The scientific-mathematical level includes all scientific theories, methods, algorithms, research, and developments necessary for the activities of the other levels. It provides the foundation for determining the expediency of creating the situation center, defines the effectiveness of its operations, integrates various components, and rectifies errors in a correct and timely manner. The engineering level provides concrete solutions in the selection and development of devices and software. It includes the necessary technological and design calculations, numerical simulations, technical equipment, facilities, program specifications, work algorithms, and so forth. The programmatic and technical levels include the appropriate support necessary for the tasks and functions assigned to the higher levels to be carried out.⁸

The main feature of the situation centers that determines their name is situational (dynamic) simulation. Prediction makes it possible to create scenarios based on analysis of the current situation and existing trends. The situation cen-

ter allows managers to see newly arising threats in a timely manner and to take measures to counter them.⁹

THE VNIPO SITUATION CENTER

The VNIPO Extreme Situation Modeling Center (Situation Center) was established at VNIPO in 2006 based on the requirements of the Concept for the Creation of the National Crisis Management Center. Functionally, the center is a part of the NCMC. The VNIPO Situation Center is designed to provide informational, analytical, and expert support for management decisions by officials from operations management agencies in responding to major fires and technogenic emergencies at critically important sites. The center's primary tasks are as follows:

- Collecting, accumulating, and analyzing information on the status of facilities at risk of fire or explosion and on EMERCOM forces, means, and reserves
 - Providing informational, analytical, and expert support for management decisions on preventing and eliminating the consequences of fires and technogenic emergencies
 - Predicting the development of fires and technogenic emergencies at critically important facilities
 - Developing, implementing, and supporting software systems for management and modeling at the Situation Center
 - Providing technical documentation for numerical simulation packages for fires and emergencies and organizing and supporting work to develop models and methodologies to facilitate the Situation Center's activities
 - Organizing the operations and information security of the Situation Center
 - Developing and supporting technical and telecommunications services at the Situation Center and developing and maintaining informational support for data banks and databases

Based on its purpose, functions, and tasks, an organizational-technical structure including the following components has been proposed for the VNIPO Situation Center:

- Analysis
- Applied software support
- Information infrastructure
- General-purpose software and hardware environment
- Complex of special-purpose software and hardware resources
- Information security subsystem

SUBSYSTEM FOR INFORMATION SUPPORT FOR MANAGEMENT DECISION MAKING

The Situation Center's subsystem for information support for management decision making must be responsible for preparing guidelines and statistical information needed for making command decisions. Databases that have been developed and are being utilized successfully lie at the foundation of the functional complexes and tasks of the information support subsystem at the Situation Center. For example, VNIPO has created a user version of the informational database "Fire and Explosive Hazards of Substances and Materials and Means of Extinguishing Them" (see Figure 5-1), which is used in more than 100 of EMERCOM's State Fire Service branches. The database contains information on more than 12,000 substances and materials, including data on the fire and explosive hazards of substances and materials, means of extinguishing them, and the potential reactions of substances and materials if they should come into contact.

VNIPO has developed and is using several regions a geographic information system for decision support in operations management by local fire and rescue units involved in responding to fires and eliminating the consequences of emergency situations. This system provides informational support for the following types of activities:

Ацетон (диметилкетон; 2-пропанон) C_3H_6O

Легковоспламеняющаяся жидкость. В воде неограниченно растворима.

$CH_3-C(=O)-CH_3$

Ацетон - Физико-химические свойства

Физико-химические свойства	
Молекулярная масса	58,08 у.е.
Плотность	790,8 кг/м ³ при 20 °С.

Ацетон - Показатели пожароопасности

Показатели пожароопасности	
Температура вспышки в закрытом тигле	-20 °С
Температура вспышки в открытом тигле	-9 °С
Температура воспламенения	-5 °С
Температура самовоспламенения	535 °С

FIGURE 5-1 Screenshot from the database "Fire and Explosive Hazards of Substances and Materials and Means of Extinguishing Them."

- Reception and processing of fire (emergency) calls, including location and formulation of orders for dispatching personnel and equipment to handle them
 - Accounting and control of the status and deployment of equipment and weapons
 - Redeployment of units, depending on their operating regimes
 - Management of operations at the fire (emergency), establishment according to proper procedure of accounting of situation changes and use of personnel and equipment, and registration of necessary information
 - Implementation of other measures aimed at ensuring service delivery according to established procedure and increasing the effectiveness of firefighters' actions

An automated decision support system for use by fire captains at the scene has been developed to provide operational information and analytical support for decision makers. This system automates the following processes:

- Accumulation and storage of site data
- Presentation in convenient form of information used by the fire captain in preparing operational decisions on managing firefighters' actions at the scene
 - Calculation of potential fire situations
 - Calculation of personnel and equipment needed to extinguish fires
 - Calculation of delivery systems for means of extinguishing fires, including calculation of pump-hose system parameters
 - Preparation of typical command decisions
 - Preparation of operational documents
 - Creation and correction of databases

SUBSYSTEM OF ANALYTICAL SUPPORT FOR MANAGEMENT DECISIONS

The subsystem for analytical support of management decisions must facilitate numerical simulation and prediction of the development of fires and emergency situations. With the aim of studying major fires at dangerous production facilities or in population centers, a series of studies has been conducted to simulate major fires in open spaces.¹⁰ Based on this research, a numerical simulation has been proposed for the aerodynamics of the environment. It is based on nonstationary Navier-Stokes differential equations, taking into account the effects of turbulence, atmospheric stratification, smoke aerosol diffusion, and phase transitions caused by the presence of moisture in the surrounding air. Figure 5-2 depicts a smoke cloud formed over a fire with a radius of 5 kilometers and a maximum heat transfer of $q_m = 4.7 \cdot 10^4 \text{ W/m}^2$.

For several decades, the institute has been working to develop and apply

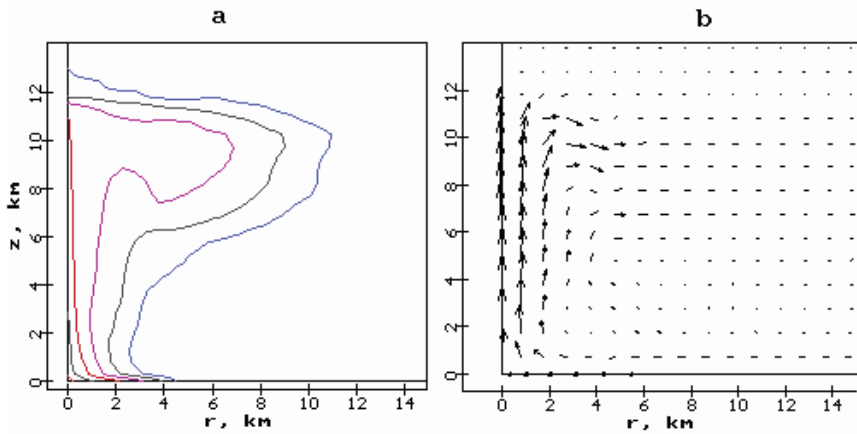


FIGURE 5-2 Isolines of smoke aerosol concentrations (a) and convective flow structure (b) over a fire with a 5-kilometer radius 1 hour after ignition.

mathematical modeling of fires in structures and buildings. Mathematical models are widely used in resolving questions of ensuring the safety of people during fires, designing evacuation paths, and creating fire alarm systems. The various mathematical models of fire development in structures (interior fires) fall into the following three categories:¹¹

1. Integral mathematical models (first-generation models)
2. Zone mathematical models (second-generation models)
3. Field (computational fluid dynamics) mathematical models (third-generation models)

Integral fire models are limited to recording physical heat parameters at the level of average values (by volume or by heat-absorbing surfaces).¹² Equations on the development of a fire describe the change in average volume parameters for the situation over time. The system of differential equations for the balance in the structure includes equations on the material and oxygen balance, equations on the balance of combustion products and inert gas, and an energy equation.

An example of the successful use of the integral modeling method would be the study conducted by institute specialists of possible development scenarios for the fire caused by the crash of a Boeing-767 aircraft into the World Trade Center in New York City. Several fire scenarios were considered. The first group of scenarios simulated the combustion of jet fuel spilled from the plane's fuel tanks, the second group of scenarios covered the burning of office furniture, and the third group focused on the combined burning of jet fuel and furniture. Figure

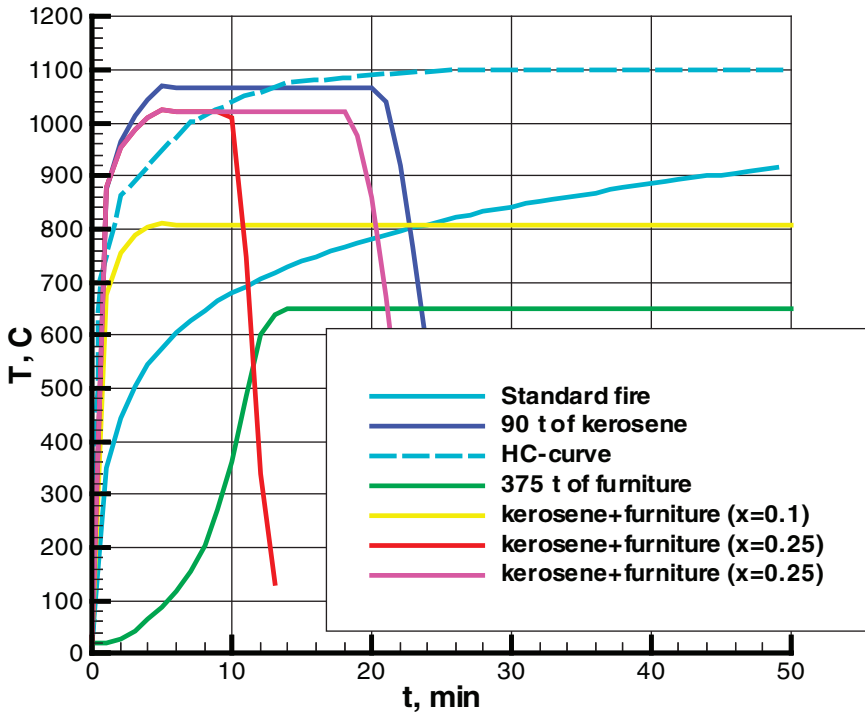


FIGURE 5-3 Calculated dynamics of average volume temperature in a structure with various amounts of jet fuel.

5-3 shows the calculated dynamics of the average volume temperature in the structure given various amounts of jet fuel assumed in the fuel load.

Based on the results of calculations of the joint combustion of spilled jet fuel and furniture, a quantitative estimate was made of the amount of fuel involved in the fire at the World Trade Center. This assessment agrees with the data from American researchers on the quantity of fuel onboard the planes just before impact.

The development of a fire may be described in more detail with the help of zone models, which are based on the premise of the formation of two layers in a burning structure: (1) the upper level of combustion products (smoke-filled zone) and (2) the lower level of undisturbed air (free zone). Thus, the status of the gaseous environment in zone models is evaluated through the use of average thermodynamic parameters from not one but several zones, and the zone boundaries are generally considered movable.

Zone models became widespread in simulating local fires in structures and

systems of structures with relatively simple configurations and having comparable linear sizes.¹³ However, creating zone models requires making a large number of simplifications and omissions based on a priori suppositions on flow structure. Such a method is inapplicable in cases where information on this structure that might be obtained experimentally is lacking, so consequently, there are no grounds for zone modeling. Furthermore, more detailed information is often required on the fire than just average parameter values for each layer (zone).

Field (computational fluid dynamics) models are more powerful and universal tools than zone models, inasmuch as they are based on a completely different principle. Several computer programs are currently available for field modeling, and they are fairly accurate in describing the rate, temperature, and concentration fields at the initial stage of a fire.¹⁴

Therefore, the field model is the best means of approaching fire modeling in complex and unique structures, for example, in transport tunnels. Figure 5-4 presents optical density fields for smoke in a central vertical section of the Lefortovo Tunnel, which is shallowly situated in Moscow's third transport ring. A study was carried out using a three-dimensional field model to predict the distribution of fire hazard factors in the tunnel both with and without antismoke ventilation.¹⁵ A traffic accident involving a truck and several passenger vehicles in this 18.2 × 5.2-meter tunnel served as the emergency situation for the purposes of the model. In this scenario, maximum theoretical heat exchange intensity of 100 megawatts was reached 15 minutes after the start of the fire. It was supposed that the fire would break out at the center of the tunnel; therefore, given the symmetry, one-quarter of the actual tunnel volume was modeled. Calculations in the model covered 750 meters of the tunnel's length.

The temperature fields in the horizontal section at the height of 1.7 meters are presented in Figure 5-5. It is clear that despite the smoke filling the evacuation paths, the temperature in the working zone up to the 240-second mark does not exceed the critical level of 343 kelvins. Smoke with a temperature of 343 kelvins reaches the height of 1.7 meters at the 300-second mark (Figure 5-5e). At this moment, the distance from the center of the fire at which the evacuation path is blocked because of increased temperature is 90 meters.

Work on simulating fires at various types of facilities holds a significant place in prediction efforts at VNIPO. Facilities involved in extracting, processing, and storing flammable and highly flammable liquids face a high risk of fire. In this regard, the institute has developed a software package to calculate fire and explosion hazard factors at such facilities. This software is intended for quantitative calculation of hazard factors and their consequences; visualization of calculation results in map format; and electronic communication of the results in the form of graphs, maps, and tables. Figure 5-6 presents a sample screenshot from this program.

In addition to its work on predicting the development of fires and emergency situations, the VNIPO Situation Center is also developing numerical simulations

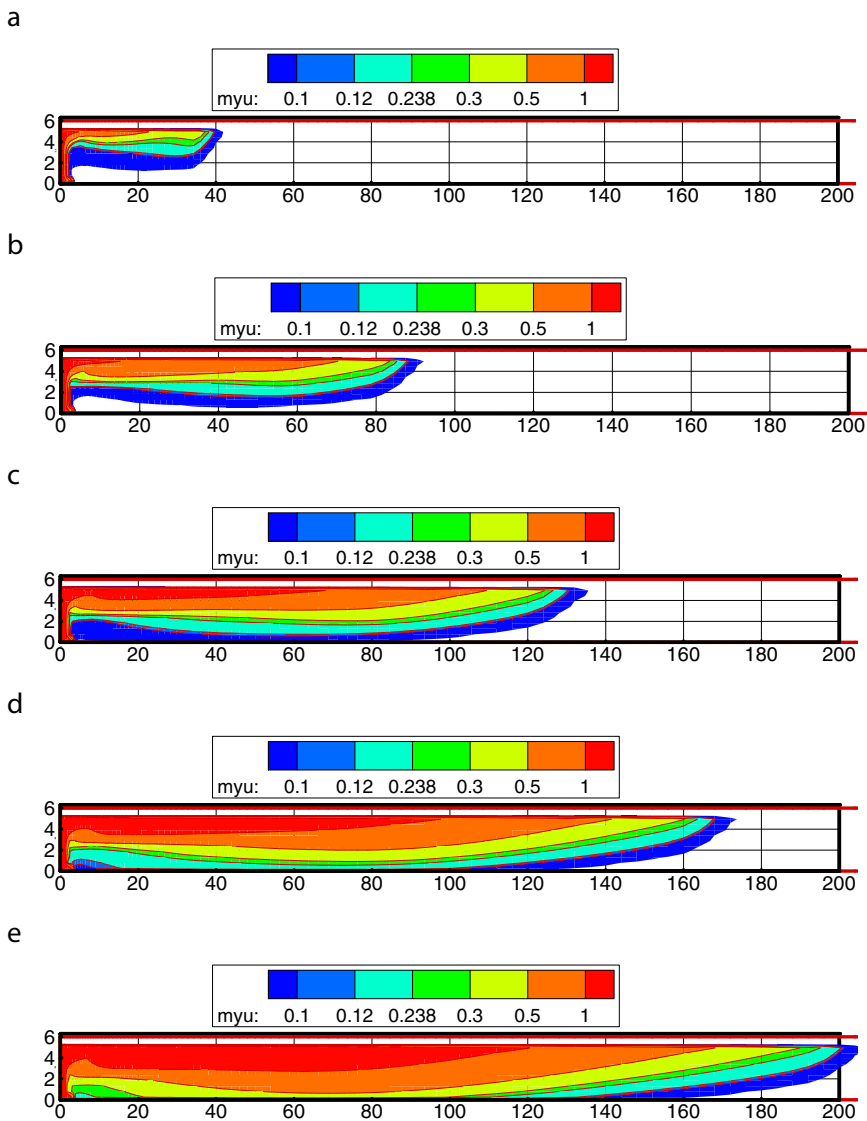


FIGURE 5-4 Optical density fields for smoke in the central vertical section of the Lefortovo Tunnel at 60 (a), 120 (b), 180 (c), 240 (d), and 300 (e) seconds after combustion.

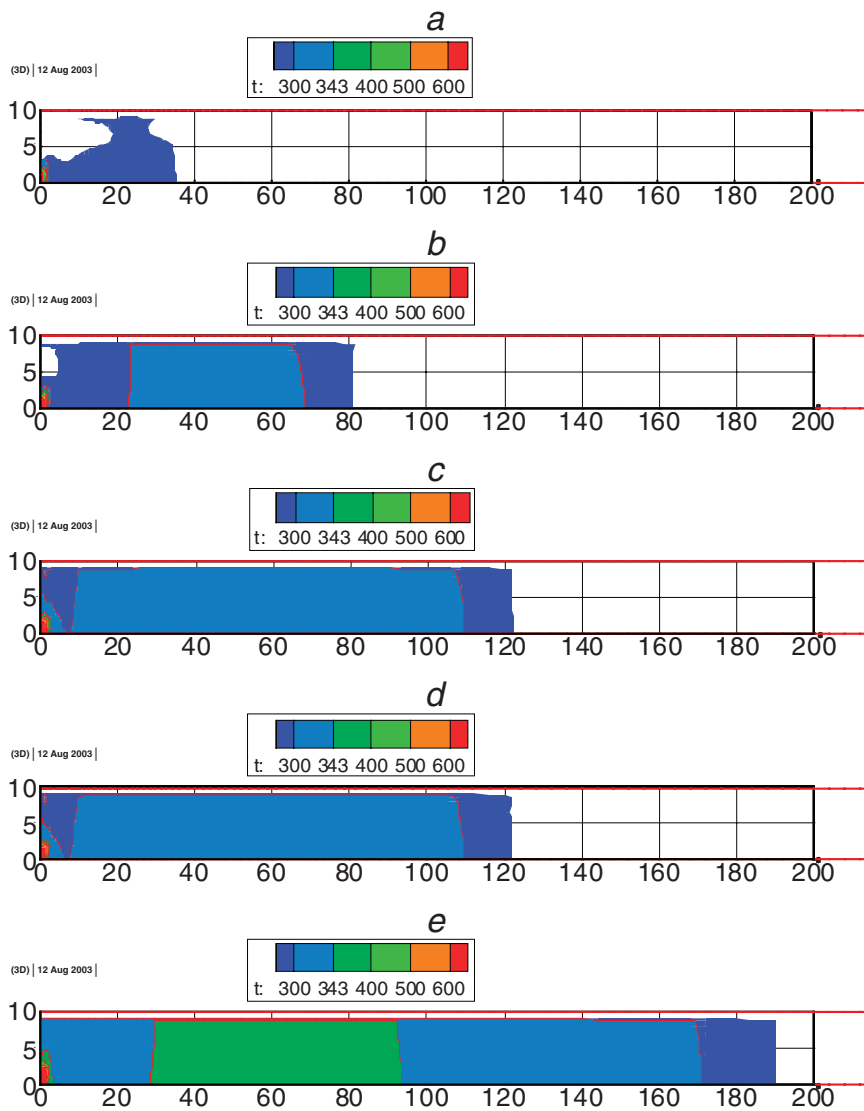


FIGURE 5-5 Temperature fields (in degrees kelvin) in a horizontal section at a height of 1.7 meters at 60 (a), 120 (b), 180 (c), 240 (d), and 300 (e) seconds after combustion.

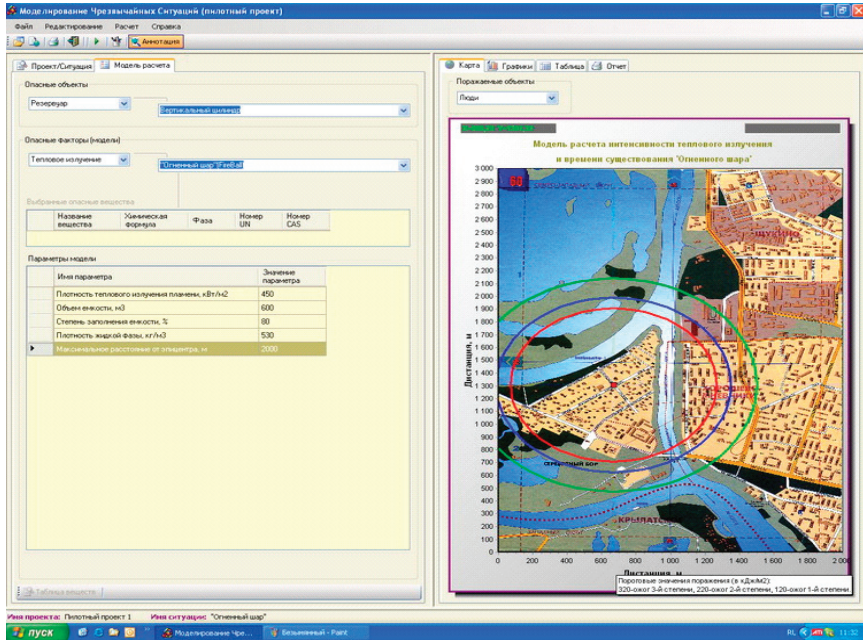


FIGURE 5-6 Sample screenshot from program to calculate fire and explosion hazard factors.

and software for process simulation of firefighting and emergency response. For example, the institute has developed a software package for calculating the personnel and resources needed to extinguish fires involving oil, petroleum products, chemicals, and stable gas condensate in storage tanks, during pour-offs to storage ponds or transfers to railway tankers, and at technical pumping stations. The program takes into account the volumes and structures of the combustion sites, the properties of the flammable liquids, tactical and technical characteristics of the foam and water delivery equipments used in extinguishing fires involving oil and petroleum products, and the characteristics of stationary and mobile firefighting equipment.

CONCLUSION

Despite existing developments in the numerical simulation of fires and emergency situations, serious issues remain to be resolved with the use of mathematical models in the work of the VNIPO Situation Center. Based on an analysis of possible fire and emergency scenarios, a list of models in need of further refinement should be drawn up, and the need for creating new models should

also be evaluated. After the models are selected, a series of studies needs to be carried out to verify them. A significant volume of work is also needed to adapt mathematical models for use in the Situation Center and to create algorithms and software packages.

Making calculations to forecast fires and emergency situations is impossible without reliable data inputs on facilities. Data collection efforts must be organized and carried out, the information must be processed, and modern technologies and geographic information systems must be used to create a database on facilities at risk of fire and explosion. In using mathematical models of fires and emergency situations based on nonlinear, nonstationary, three-dimensional model systems (for example, field models of fires), it should be taken into account that numerical solution of such systems requires tens of hours of computer time even using high-output processing technologies.

Introducing new modern technologies for numerical simulation of emergency situations requires the following:

- Improving the reliability of predictions to prevent and eliminate the consequences of emergency situations
 - Organizing comprehensive monitoring and information-processing efforts regarding the status of facilities, the environment, and natural and technogenic phenomena that cause emergency situations
 - Developing mathematical models of the development of fires and emergency situations
 - Optimizing and facilitating timely correction of action plans and measures for preventing emergency situations as well as eliminating their consequences
 - Providing a modern level of technical capabilities to support the work of operations personnel, including network communications technologies and means of collecting, analyzing, and presenting information on emergency situations

NOTES

1. *Technogenic* is used to refer to phenomena arising as a result of the development or deployment of technology.
2. Vorobyov, Yu. L. 2005. *Safety in Daily Activities (Aspects of State Policy)*. Moscow: Business Express, 376 pp.
3. Faleev, M. I. 2002. Computer technologies in creating an information space for dealing with disasters and catastrophes. *iBUSINESS* 6:19-21.
4. Concept for the Creation of the National Crisis Management Center. 2005. Moscow: Ministry of the Russian Federation for Civil Defense, Emergencies, and Elimination of Consequences of Natural Disasters, 35 pp.
5. National Crisis Management Center.

6. Shatrov, V. F., and A. Yu. Silantyev. 2003. Situational centers: Information support for high-level management decisions. Pp. 8-17 in *Systems Problems of Quality, Mathematical Modeling, and Information and Electronic Technologies—Part II: Imitative Modeling and Conflictology. Materials from an International Conference and the Russian Scientific School*. Moscow: Radio and Communications.
7. Filippovich, A. Yu. 2003. *Integration of Situational, Imitative, and Expert Modeling*. Moscow: Radio and Communications, 310 pp.
8. Filippovich. *Integration*.
9. Romanov, V. V., and D. D. Shulga. 2003. Conceptual description of conflicting interactions. *Strategic Stability* 2:16-21.
10. Kopylov, N. P., A. M. Ryzhov, and I. R. Khasanov. 2000. Major fires and their modeling. Pp. 170-187 in *Modeling fires and explosions*, N. N. Brushlinsky and A. Ya. Korochenko, eds. Moscow: Pozhnauka [Fire Science].
- Kopylov, N. P., and I. R. Khasanov. 2001. Predicting the fire situation at sites under demolition. Pp. 101-102 in *Extreme Situations: Prevention and Elimination. Collected Materials from a Scientific-Practical Conference*. Minsk: Belarus State University.
11. Ryzhov, A. M., I. R. Khasanov, A. V. Karpov, et al. 2003. *Application of a Field Method for Mathematical Modeling of Fires in Structures: Methodological Recommendations*. Moscow: VNIPO, 35 pp.
12. Astapenko, V. M., Yu. A. Koshmarov, I. S. Molchadsky, and A. N. Shevlyakov. 1988. *Thermodynamics of Structure Fires*. Moscow: Stroiizdat [Construction Publishers], 448 pp; Molchadsky, I. S. 2005. *Fire in a Structure*. Moscow: VNIPO, 456 pp.
13. See, for example, Cooper, L. Y., J. A. Rockett, H. E. Mitler, and D. W. Stroup. 1989. A program for the development of a benchmark compartment fire model computer code. *Fire Technology* 25(4):116-127.
- Takeda, H. 1988. Transient model of early stages in compartment fires. Pp. 21-34 in *Mathematical Modeling of Fires*, J. R. Meffaffey, ed. Philadelphia: ASTM; Merkushkina, T. G., and V. V. Romanov. 1981. Use of mathematical modeling in studying fire hazard factors. Pp. 34-43 in *Safety of People in Fires*. Moscow: VNIPO.
14. Ryzhov et al. *Mathematical Modeling of Fires*.
- Ryzhov, A. M. 2000. Field models of fires. Pp. 25-88 in *Modeling Fires and Explosions*, N. N. Brushlinsky and A. Ya. Korolchenko, eds. Moscow: Pozhnauka.
- Yang, K. T., J. R. Lloyd, A. M. Kanury, and K. Satoh. 1984. Modeling of turbulent buoyant flows in aircraft cabins. *Combustion Science and Technology* 39:107-118.
- Raycraft, J., M. D. Kelleher, H. Q. Yang, and K. T. Yang. 1990. Fire spread in a three-dimensional pressure vessel with radiation exchange and wall heat losses. *Mathematical and Computer Modeling* 14:795-800.
- Cox, G. 1995. *Combustion Fundamentals of Fire*. London: Academic Press, 476 pp.
- Welch, S., and P. Rubini. 1996. *SOFIE—Simulations of Fires in Enclosures: User Guide*. Bedford: Cranfield University, 127 pp.
15. Ryzhov et al. *Mathematical Modeling of Fires*.

Organizational Measures and Decision Support Systems for Preventing and Responding to Terrorist Acts at Potentially Hazardous Facilities, on Transportation Systems, and in Locations Where Large Numbers of People Congregate*

*A. Yu. Kudrin, Director, All-Russian Scientific Research Institute for Civil Defense and Emergency Situations (ICDES) (Federal Center);
A. I. Zaporozhets, Deputy Director for Research, ICDES; and
S. A. Kachanov, Deputy Director, ICDES*

Terrorism is a complex, multifaceted phenomenon that is social in nature and, in some instances, has a political aim. Terrorists attempt to exert political pressure on government leaders, attract world public attention to certain problems, demand the liberation of arrested supporters of extremist groups and the end of persecution of terrorist organizations and their leaders by law enforcement agencies, advance economic demands, and so forth.

As a rule, terrorists commit individual acts of an intentionally provocative nature, which may include threats of murder or the assassination of state and political figures; the seizure of hostages or potentially hazardous facilities; bombings; or the release of poisons, radioactive substances, or biologically active agents. This will lead to deaths among members of the public who happen to be at the site of the attack and will harm the economy and the prestige of the state.

Terrorist acts at potentially hazardous facilities—enterprises working with chemicals, radioactive materials, or explosives; hydrotechnical structures; unique tall buildings; subways, surface rail, and air transport facilities; and places where large numbers of people congregate, such as concert halls, stadiums, apartment

*Translated from the Russian by Kelly Robbins.

buildings, and so forth (hereafter referred to as facilities)—present a great danger to personnel and the public and cause substantial economic damage. Terrorist acts at enterprises could be carried out by striking (destroying) a tank or pipeline holding catastrophically hazardous chemicals, a nuclear reactor, or a storage vessel containing highly flammable liquid. An explosion at a chemical-hazard facility could cause destruction over an area of up to 30 square kilometers, with the number of injured victims possibly reaching 60,000 and up to 5,000 fatalities. Destruction of an atomic reactor could contaminate up to 1,200 square kilometers, with the number of casualties in this situation possibly reaching 10,000.

If a terrorist strike against a hydrotechnical structure were to occur, we might expect cities or towns to be flooded and buildings to be destroyed by the resulting surge of water. The land area submerged could reach about 1,000 square kilometers, with the number of victims possibly reaching 120,000.

In places where large numbers of people gather, terrorists could use explosives, dangerous chemicals (including poisons), radioactive substances, and biologically active agents.

The suddenness of a terrorist act, the rapid spread of the impact factors, the deaths of many people, the ensuing panic, and people's sense of being unprotected create a powerful psychological blow to society. Therefore, prompt response to a terrorist threat or act is an important factor in preserving the lives and health of people subjected to such attacks. Many organizations of various types have been involved in studies on preventing and eliminating the consequences of terrorist acts. The Russian Ministry for Civil Defense Affairs, Emergencies, and Elimination of Consequences of Natural Disasters (EMERCOM) is responsible for emergency rescue and other urgent efforts involved in eliminating the consequences of terrorist acts.

A unified state system for emergency situation prevention and response has been created and is operating in Russia. Within the boundaries of specific jurisdictions, administrative agencies specially empowered to handle issues related to protecting the public and area from emergency situations, depending on the circumstances and scope of the predicted or actual situation, establish one of the following operating regimes for the subsystems of the unified state system for emergency management:

- Standard daily operating regime: during normal production activities in the absence of any predictions of possible terrorist acts
- Increased readiness regime: when possible terrorist acts are predicted at a facility
- Emergency regime: when a terrorist act has been committed at a facility

Basic measures involved in the standard daily operating regime are as follows:

- Situational observation and monitoring at facilities and adjacent areas by facility staff and law enforcement personnel
- Organization and implementation of training for local government and law enforcement personnel, facility staff, the public, and emergency rescue personnel in means of protection and appropriate actions to be taken at a facility, on a transport system, and in open spaces if a terrorist act is committed
 - Planning, organization, and implementation of training exercises on emergency warnings, protection of people against the effects of impact factors, and reduction of losses and damage from a terrorist act
 - Participation in the development and implementation of organizational and engineering-technical measures to ensure more stable operations of facilities and transport systems in an emergency resulting from a terrorist act
 - Creation and augmentation of stores of emergency supplies and monitoring of the usability of individual protective gear; medical supplies for individual protection; and equipment needed for communications, public notification, and chemical, radiation, and biological surveillance and monitoring
 - Organization of matters regarding the interactions of special emergency response subunits with EMERCOM, the Ministry of Internal Affairs, the Ministry of Communications, the Federal Security Service, the Ministry of Healthcare and Social Development, the Ministry of Defense, and other Russian ministries and departments
 - Cooperation with local government agencies and officials specially authorized to deal with combating terrorist acts in order to select sites for decontamination stations for equipment and clothing, sanitary washing stations, and accumulators (observation stations) for eliminating the consequences of terrorist acts at facilities that involve the use of dangerous chemicals (poisons), radioactive substances, and biologically active agents
 - Training of personnel from EMERCOM specialized subunits and facility staff on actions to eliminate the consequences of terrorist acts, including victim assistance and use of technical means for containment, special processing techniques using equipment, and sanitary processing of individuals
 - Other matters aimed at preventing losses and reducing damage from a terrorist act in accordance with the specific characteristics of operations at each particular facility

Basic measures involved in the increased readiness regime are as follows:

- Assumption by the appropriate emergency commission of direct operational command of the emergency management system subunit functioning at the site of the terrorist act; formation of operations groups at the local level to ascertain the situation at the site of the terrorist act; and provision of effective assistance to facility staff and law enforcement personnel in dealing with the emergency

- Communication of the threat (prediction) of an emergency situation to the appropriate Russian Federation ministry, department, or organization with jurisdiction
 - Notification of facility staff and law enforcement personnel at the facility about the terrorist act
 - Testing of operational communications and clarification of interactions between the appropriate emergency commission and the EMERCOM crisis management center
 - Augmentation of security and dispatch services at the facility
 - Increased observation of the situation at the facility and in adjacent areas
 - Distribution of individual respiratory protective gear to be kept at the ready by facility staff and law enforcement personnel
 - Preparation of portable and mobile devices for chemical, radiation, and biological surveillance and monitoring for use if needed
 - Placement of EMERCOM personnel and resources at the appropriate level of readiness; clarification of plans for their actions

Basic measures involved in the emergency regime are as follows:

- Clarification of the situation in the zone where the terrorist act occurred
 - Notification of officials specially authorized for involvement in combating terrorist acts, facility staff, and law enforcement personnel that a terrorist act has been committed
 - Conduct of overall survey (chemical, radiation, or biological, as needed) and monitoring efforts to establish whether explosives, hazardous chemicals (poisons), or biologically active agents were used; establishment of perimeter of zone impacted by explosives, affected by chemicals (poisons) or biological agents, or contaminated by radioactive substances
 - Evacuation of the public from the danger zone
 - Distribution of individual protective gear to victims (if necessary)
 - Provision of initial medical and paramedical assistance to victims
 - Execution of measures to eliminate the source of the emergency
 - Execution of measures to decontaminate the area; specially process individual protective gear, uniforms, and equipment; and provide sanitary processing for personnel involved in containing and eliminating the consequences of terrorist acts in which dangerous chemicals (poisons), radioactive substances, or biologically active agents were used

Based on an analysis of likely threats that could lead to emergency situations, individualized security systems must be developed for industrial enterprises, unique tall buildings, facilities where large numbers of people gather, and subway

stations. Such systems should take into account natural, technogenic, biological, social, and terrorist factors that could cause emergency situations. Such security systems include both organizational and technical measures. Organizational measures provide plans for the actions of personnel, residents, and facility visitors both in regular day-to-day activities and during emergencies, threats of terrorist acts, and such acts themselves. They are laid out in the appropriate regulatory technical documents. Plans for rescuing and evacuating people and eliminating the source of the emergency should be developed in a timely fashion through training exercises and courses.

Technical measures are developed with the aim of supporting the normal functioning of a facility under its regular daily operating regime, during threats, and during actual emergencies. These measures are implemented using engineering and technical means: design and structural elements; barriers; blocking devices and mechanisms; security, fire alarm, and warning systems; systems for monitoring and management of facility security and critical operations; loudspeakers and other means of notification; video observation systems; means and systems for facility access control and management; environmental monitoring equipment; and so forth.

All facilities must be prepared for an emergency. To achieve this, measures are taken to improve the facility's level of protection. The list of measures could be augmented and revised depending on the facility's function.

Critically important points are identified in the design stage. When the facility is in operation, access to these points is limited and they are constantly monitored. Such points include structural elements that, if destroyed, would lead to destruction of the entire facility, as well as technological systems and equipment that, if affected by an accident, could lead to an emergency situation. Physical protection boundaries are organized and equipped with monitoring rooms, alarm systems, controlled access points, and inspection points for vehicles and individuals. The necessary badges or access cards are distributed to staff. An accounting is made of residents and visitors. Regulatory technical documents on actions to be taken in an emergency and systems for communications with supervisory agencies and fire and rescue personnel are developed and forwarded to those responsible for implementation. Special attention is devoted to seeking and detecting unauthorized persons and objects, finding them in a timely manner, and handing them over to law enforcement personnel or specialists. Personal cars and trucks with compressed gas-powered engines are prohibited on the grounds of the facility. The number of persons involved in facility access control and monitoring is increased.

As for preventing and eliminating the consequences of emergency situations at facilities, much attention is currently being focused on automated systems used there. The All-Russian Scientific Research Institute for Civil Defense and Emergency Situations (ICDES) has developed an original technology and the necessary regulatory and methodological base for creating automated interconnected

security and utility systems and structured systems for monitoring and managing engineering systems at buildings and structures. The technology that has been developed makes it possible to prevent or significantly reduce the consequences of emergency situations caused by critical utility failures; the sudden collapse of structural elements of buildings and other structures; fires; explosions; increased levels of hazardous chemicals, radiation, or biologically active substances; or terrorist acts.

The programmatic and technical solutions that have been developed make it possible to

- support the operations of all security and critical utility systems according to previously determined algorithms in emergency situations, including those caused by terrorist acts;
- facilitate the uninterrupted, remote, real-time, automated processing of information on the status of critical utility and security systems and engineering-technical elements at facilities and automatically transmit the necessary data on the parameters of the emergency in an established format to the necessary response service; and
- facilitate long-distance management of critical utility and security systems at facilities from a remote control center in the city in emergency situations, including those caused by terrorist acts.

Preliminary calculations indicate that the creation of this system would reduce the number of emergency situations in buildings and structures by at least 20 percent and would cut materials losses by more than 15 percent.

To prevent the sudden collapse of buildings and structures, the institute has developed a technology for remote monitoring of engineered technical elements. Two parameters are monitored: (1) individual fluctuation periods (frequencies) of barrier elements and (2) displacements (vertical, horizontal, and twisting). The data obtained are then automatically processed mathematically, resulting in output on the condition of the structural elements of the facility (normal, increased attention, or alarm). The results of the monitoring are automatically transmitted to the necessary response services.

With the aim of preparing scientifically grounded recommendations on actions to be taken in emergency situations, including those caused by terrorist acts, the Center for Decision Support in Emergency Situations has been created at ICDES. The center has the necessary software allowing it to determine automatically the scope of a given emergency and to prepare the necessary recommendations on rescue and other urgent efforts to save people and minimize material damages. The software was created on the basis of existing packages and well-proven methodologies. Measures to prevent and respond to emergencies are being prepared not only on the basis of theoretical tasks but also using accumulated knowledge bases such as previous experience in carrying out such

efforts, new methods and technologies for eliminating the consequences of various types of emergencies, data on new emergency rescue tools and their availability, and so forth.

Specialists from other ministries and departments could be involved in preparing recommendations, including by means of videoconferencing.

The center's preparation of timely, scientifically grounded recommendations on preventing and responding to various types of emergency situations makes it possible to reduce substantially the likelihood of a disaster at facilities and to save significantly more people and reduce the costs of rescue efforts if such situations do occur, including those caused by terrorist acts.

International and National Priorities in Combating Terrorism in the Transportation Sector

*Vladimir N. Lopatin,
Republic Scientific Research Institute of Intellectual Property*

Despite the increasingly systemic and organized efforts of the international community and individual states, terrorist threats continue unabated. In an effort to inflict the most serious damage and intimidate the government and people, terrorists select the most vulnerable targets for their attacks.

BACKGROUND

To strengthen the fight against terrorism and improve its effectiveness, 7 years ago we Russian scientists concluded that it made sense to focus antiterrorist activities not only on critical areas particularly dangerous from the standpoint of the threat of terrorist attacks but also on especially critical facilities. These primarily include transport, which, because of its transnational nature, serves as (1) an environment for “economic” activities of international terrorist and other criminal groups, (2) a target for banditry, or (3) a means for the perpetration of terrorist acts. Although up to 70 percent of terrorist acts are either committed on transport or involve its use, this has not been reflected adequately in legislative or law enforcement practice.

Following analysis of the situation in Russia and in the Commonwealth of Independent States (CIS) as a whole both at the international conference “Terrorism and Transport Security” held in Moscow on February 5-6, 2002, and

subsequently, experts identified a number of reasons why transportation may be categorized as a critical target:

- Sharp increase in hazardous cargo as a proportion of the total volume of goods transported
- High level of infrastructure decay and high accident rate in the transport sector
- Relative accessibility
- Use of smuggling by transnational criminal groups as a source of financing for terrorism
- Possibility of attracting broad public and media attention
- Association with national symbols (national airlines)
- Possibility that even a single act or attack will immediately affect many people

For these reasons, security and crime prevention in the transport sector is one of the priorities of the state and society.

Based on an analysis of legislation and law enforcement practices in 2000-2001, it was clear that transport policy did not include an antiterrorism component, and antiterrorism activities did not focus on transport. There was very little overlap between these two sectors. At that time we were asked to define a priority area in transport policy, namely, ensuring security and antiterrorism activities, and to create a similar focus on the transport sector as a priority area in antiterrorist activities. The CIS Transportation Coordinating Council agreed with this assessment in the Chisinau Declaration on Transportation Safety, as did the Council of Ministers of the European Conference of Transportation Ministers in its closing document and in the Bucharest Declaration on Combating Terrorism in Transport on June 6, 2002. This approach is also reflected in a statement on the fight against terrorism in the transport sector adopted on June 28, 2002, at the summit of the Group of Eight (G-8) in Kananaskis, as well as in subsequent decisions of international and state structures. Further evidence that the first steps have been taken in developing this consciousness and understanding may be seen in subsequent years when the first intergovernmental agreement on transportation safety was adopted, including a set of principles and mechanisms for implementing state policy on transportation security and counterterrorism. Another important step was the adoption in 2006 of the Federal Law on Transportation Security. A comprehensive and systematic approach to these problems is reflected in the CIS Intergovernmental Program of Joint Measures for Combating Crime in 2005-2007 and in cooperative programs among CIS member states for fighting terrorism and other extremist phenomena in 2005-2007 and countering the illicit drug trade.

Thus, the problem of understanding and awareness at the level of experts, academics, and individual government officials and business leaders has today reached the level of government and international understanding, which has been

reflected in specific decisions made by state authorities and international organizations in this regard. These decisions may be considered a starting point in improving transport and antiterrorism policies and in creating on this basis an integrated new sphere of state policy: transportation security and counterterrorism.

The new approach in the formation of the counterterrorism strategy and its implementation in the transport sector is complex both in its identification of the targets and the subjects of counterterrorist activities and in the principles and mechanisms of their interaction. And today, scientists must help to take the next step in implementing this approach to promote security and counterterrorist objectives in the transport sector.

FOCUS AREAS FOR ANTITERROR ACTIVITIES

Comparing the norms of international laws to which Russia is a party with norms of Russian legislation, it should be recognized that there is currently no antiterrorist strategy on transport that would be mandatory for state structures, including both the transport complex and law enforcement, and that would take into account the specifics of all types of transport, from aviation to subway systems. It would probably be wrong even to implement a counterterrorism policy at all without making it specifically applicable to elements of the transportation sector, given its very substantial special characteristics.

An analysis of international agreements on counterterrorism suggests that of the seven major transportation modes, air and sea transport are subject to the most restrictions. The other modes are either only the subject of general mention and declarative statements or entirely absent from the list of antiterrorist activities. For example, the Concept for a Coordinated Transport Policy among CIS member states for the period through 2010, approved by decision of the Council of CIS Heads of Government on September 15, 2005, mentions only aviation, marine, river, and rail transport with regard to antiterrorism and security activities related to transport policy. Such a mention is lacking in the section on vehicular transport, while pipelines and subways are not included in the document at all.

Therefore, it remains an urgent challenge to adopt an antiterrorism strategy for the transport sector to ensure transportation security as an integral part of the international counterterrorism system. This will entail developing and making the necessary amendments to the Transport Strategy and to targeted programs for modernizing the transport system. It will also require securing allocations in the antiterrorist strategy for law enforcement to make counterterrorism on transport a priority, taking into account the specific characteristics of its seven major modes.

ORGANIZATIONS INVOLVED IN ANTITERROR EFFORTS

In addition to law enforcement, other government agencies and nongovernmental organizations must be key actors in carrying out crime prevention measures to implement United Nations Security Council Resolution 1373 of September 28, 2001, as without them this effort will be ineffective and will not produce the expected results. Preventing terrorism can and must be done through the joint efforts of all government agencies and with the support of civil society, science, and business at both the national and international levels, including in the CIS. The new conditions require new rules for interaction between government, science, and the business community in order to establish partnerships in addressing the common task of countering terrorism.

In 2001, Russian scientists found that to confront the well-armed, well-trained, and highly professional enemy that is international terrorism, it is necessary not only to combine the efforts of the various law enforcement agencies but also to promote cooperation between law enforcement and transportation agencies; the state and nonstate sectors; and government, science, and business. This initiative to unite the efforts of government, science, and business led to the establishment on May 20, 2002, of the High-Level Advisory Group on Countering Terrorism in the Transport Sector in the Russian Federation. This group includes designated representatives of State Duma committees, all transport and law enforcement agencies, transport companies, the Russian Academy of Sciences, the Russian Chamber of Commerce and Industry, the CIS Transportation Coordinating Council, and the International Road Transport Union (IRU). The following accomplishments have been made on the initiative of the group and thanks to the efforts of researchers and practitioners:

- Unique counterterrorism experience, both negative and positive, has been summarized at six international conferences on terrorism and transportation security, the results of which have been published in individual book form. In 2006, by decision of the CIS Interparliamentary Assembly, the conference was given the status of a permanent CIS advisory body on counterterrorism and transportation security.

- Recommendations of the first five international scientific conferences on terrorism and transportation security are for the most part being implemented and are finding support in the decisions of CIS intergovernmental agencies, including the Interparliamentary Assembly, the CIS Executive Committee, state agencies of CIS member countries, and the Collective Security Treaty Organization. In particular, the recommendations of the third and fourth international conferences have formed the foundation for practical efforts to protect civil aviation against acts of unlawful interference.

- A unique set of statistics was collected on terrorism in the transport sector in the Russian Federation, international and national legislation in this area

was analyzed, and in 2003 an unparalleled white paper entitled “Terrorism and Transportation Security in Russia (1991-2002)” was published.

- A list was prepared of suspicious International Road Transport (TIR) carnet (shipment log) transactions that, if encountered, should cause national road shipment associations not only to refuse to issue (withdraw) a TIR carnet but also to inform relevant law enforcement agencies (similar to efforts established to counter money laundering). In December 2002 the list was adopted as a regulation at the IRU General Assembly in Geneva, requiring compliance by all national road shipment associations in the 64 IRU member countries.

This Russian initiative was supported in the Chisinau Declaration on Transportation Safety (May 27, 2002), which was adopted at a meeting of the CIS Transportation Coordinating Council featuring the participation of all ministers of transport from the CIS member. This declaration was circulated as an official document at the European Conference of Ministers of Transport, the World Road Transport Forum (June 2, 2002), and a joint session of the CIS Interparliamentary Assembly commissions on political affairs and defense and security in the city of Astana (October 24, 2002). It was also submitted as part of the G-8 Action Plan on a Secure and Facilitated International Travel Initiative (June 11, 2004). In particular, the September 18, 2003, decision of the CIS Council of Heads of Government directly orders law enforcement agencies to work with high-level advisory groups on transportation security.

A number of issues remain unresolved, including clear definition of objectives, functions, and structures; coordination and interaction of governmental and nongovernmental entities involved in countering terrorism in the transport sector; harmonization of regulations and the activities of state security structures; and implementation of measures to ensure the efficiency and optimal utilization of mobile transport units in counterterrorism activities. In particular, it is necessary to develop and establish in regulatory form mandatory procedures for cooperation among law enforcement agencies, national associations of road transporters, and transport organizations if they detect a suspicious operation, a list of which has been drawn up and approved by both the Russian Federation and the IRU. This experience and the favorable response that this Russian initiative has elicited suggest that further progress would be possible in setting priorities for international cooperation in the fight against terrorism in the transport sector.

PRINCIPLES FOR ANTITERRORIST ACTIVITIES IN THE TRANSPORT SECTOR

Along with the well-known and generally accepted principles of cooperation, the new conditions have given rise to new rules that remain to be adopted and established in regulatory form as uniform and compulsory for all participants in antiterrorist activities at both the national and the international levels.

The first issue is how to determine the balance between the interests of development (including freedom of movement) and the interests of security, the balance between obligations to provide protection against terrorist acts and the obligation to protect human rights.

With regard to striking a balance between ensuring human rights and combating terrorism, the Guiding Principles of the Council of Europe affirm a restriction forbidding arbitrary treatment and legislation with a retroactive effect, assert the right to a fair judicial hearing, and reject extradition of individuals to countries where they may be condemned to death. This is necessary but clearly not enough.

The strategy must be aggressive and specifically set forth in legal decisions. An aggressive strategy involves making adjustments and very substantial ones in the legislative framework, including standards and principles of international law that have long run counter to today's situation and have become obsolete, beginning with the Tokyo Declaration of the 1960s and other documents adopted regarding the transport sector in the 1970s. The situation has long since changed. Absolutely new threats have arisen, and it seems to me that understanding and awareness of this will only allow us to work together to adjust international legal standards and principles in order to counter our common enemy, international terrorism, and to amend national legislation as well, thus providing a sound foundation for the offensive against terror in the transport sector both in Russia and in the world as a whole.

Second, applying experience in counterterrorism activities to other modes of transport should be done in a gradual and rational fashion. For example, efforts are under way to resolve the issue of creating a technical monitoring system that will automatically collect and format data on suspicious signs suggesting preparations for commission of a terrorist act on transport. This system would include real-time transfer of data on passengers (passport data) from all transport enterprises regardless of their form of ownership to internal affairs agencies when passengers check in for air, rail, or water travel.

Third, in the fight against terrorism it is important to be consistent in keeping and using what works. An example is the rejection of participation by internal affairs agency personnel in joint predeparture inspections along with airline security personnel and the subsequent recognition that this decision had been a mistake. A similar error was made in eliminating the presence of personnel from the public prosecutor's office on transport and at sensitive facilities, a mistake that is being rectified by the new attorney general of Russia.

Fourth is the issue of developing and implementing common standards for security, for example, standards for installing modern equipment at inspection points at airports and seaports, including devices capable of detecting explosives on the human body, thus eliminating the need for manual searches. This rule is especially true, given the many structures created and operating in this sphere (more than 30 international entities operating in Russia).

International Counterterrorism Structures

- Counterterrorism Committee of the UN Security Council (established under UN Security Council Resolution 1373 of September 28, 2001)
- Interpol
- World Customs Organization
- International Atomic Energy Agency
- International Civil Aviation Organization
- International Maritime Organization

In Europe

- Action Against Terrorism Unit of the Secretariat of the Organization for Security and Cooperation in Europe
- Europol
- European Conference of Ministers of Transport
- Eurasian Transport Union

In Asia

- UN Economic and Social Commission for Asia and the Pacific
- Eurasian Transport Union

In the CIS

- Counterterrorism Center of CIS Member States
- Coordinating Office for Combating Organized Crime and Other Dangerous Types of Crime in CIS Member States
- Coordinating Conference of Attorneys General of CIS Member States
- Council of Heads of Security Agencies and Special Services of CIS Member States
- Council of Ministers of Internal Affairs of CIS Member States
- Council of Ministers of Defense of CIS Member States
- Council of Commanders of Border Forces of CIS Member States
- Council of Heads of Customs Services of CIS Member States
- Council of Ministers of Foreign Affairs of CIS Member States
- Transportation Coordinating Council of CIS Member States

Fifth is the issue of the transition from departmental and then program-based planning to targeted project-oriented planning, financing, and management, including for antiterrorist activities in the transport sector. This requires the development of a system of indicators regarding the main subjects of antiterrorist activity. Upon analysis of the summary report on the results and main activities

of the government of the Russian Federation for 2006-2008, it is possible to state that such a system does not exist (the report's section on transportation security features only two indicators for assessing the activities of government agencies regarding air transport). The task of scientists is to help the authorities detect and recognize problems and find ways of solving them. To ensure that scientific recommendations form the basis for improvements in the future work of state and nongovernmental structures and organization of interactions between them, it is important to follow the principle of joint operation, working together instead of trying to replace one another.

Characteristics of Technological Terrorism Scenarios and Impact Factors*

*Nikolai A. Makhutov, Vitaly P. Petrov, and Dmitry O. Reznikov,
Russian Academy of Sciences Institute of Machine Sciences*

INTRODUCTION

Technological terrorism is defined as actions directed against infrastructure elements critically important for national security or committed with the use of especially hazardous technologies, technical means, and materials. In considering technological terrorism scenarios, the primary impact factors of such terrorist acts initiate secondary catastrophic processes with a significantly higher (tens and hundreds of times) level of secondary impact factors that affect the targets of the attack, their personnel, the public, and the environment.

The scope and intensity of the impact factors of terrorist actions against a given system define the level of the terrorist threat to that system.

The scenario for a terrorist attack entails a means of exerting the initiating effect on the system that is based on the use of appropriate technical devices, technologies, and materials and is characterized by the terrorists' deliberate selection of the place and time of the attack.

The following characteristics must be taken into account in analyzing technological terrorism scenarios and impact factors.¹

*Translated from the Russian by Kelly Robbins.

High level of dynamism: Terrorist attack scenarios and impact factors are more dynamic in nature than scenarios and impact factors for natural and technogenic² disasters to which the system is subject. Of course, emergency management and evacuation capabilities are relevant to both. A change in the spectrum and intensity of possible terrorism-related extreme effects on the system is significantly more powerful than a natural or technogenic threat. This is due to the terrorists' capacity for constantly expanding their arsenal of mechanisms for initiating emergency situations using modern means of attack, reacting to changes in protection systems, and drawing lessons from mistakes made during previous attacks on the system or others like it.

High level of uncertainty: In modeling terrorist scenarios and impact factors, we encounter a higher level of uncertainty. In addition to the undefined factors inherent in threats of a natural or technogenic nature, terrorist threats entail new factors of uncertainty resulting from the complexity of evaluating terrorists' value system and behavioral logic as well as their organizational-technical potential and the resources at their disposal.

Capability of terrorists to choose attack scenarios deliberately: This refers to terrorists' deliberate selection of attack scenarios (places, times, and types of actions), taking into account system vulnerability parameters and the damages expected if an attack is successfully carried out. That is, terrorists are capable of analyzing the vulnerability matrix and damage structure for various types of actions against a system and selecting the attack scenario that maximizes the harm to society (taking secondary and cascade damages into account). Here, in addition to probability analysis, it is also necessary to apply the tools of game theory, which makes it possible to take the intentional actions of terrorists into account.

Characteristics of the perception of the terrorist threat: A significant part of the population is inclined to fear terrorist attacks to a greater degree than equivalent natural and technogenic phenomena as described in the equation $R = H^n \cdot V \cdot U$ where $n < 1$, the indicator for the degree characterizing the subjective perception of the consequences of terrorist acts.

Complex nature of the terrorist threat: The presence of a terrorist organization in a region may give rise to the possibility of a broad spectrum of attack scenarios, including the time, place, and character of the attack. Thus, to counter terrorist threats and terrorist mechanisms for initiating emergency situations to an even greater degree than for natural and technogenic risks, a complex systems approach is needed for ensuring security and developing an optimal strategy for counterterrorism force and resource deployment. Inasmuch as concentrating resources on protecting one system element (or protecting a target from one type of terrorist action) could prove useless because, after evaluating the situation, the terrorists could either redirect the attack against another element of the target or could switch to a different type of attack. In this case, counterterrorism efforts will not lead to reducing risk and increasing the target's level of protection.

In addressing traditional tasks of ensuring security against natural and tech-

nogenic disasters, the prevailing types of impact factors could be highlighted for the system being studied, such as threats from seismic activity, flooding, chemical contamination, and so forth. In protecting the system from these impact factors, it is possible to achieve the desired result. However, in protecting a given system from manifestations of terrorism, the spectrum of potential threats is significantly wider. Here, terrorists are capable of analyzing the level of protection of the system for various types of impact factors, identifying impact factors against which the target is least protected, and concentrating their efforts on carrying out an attack that will bring these very factors to bear.

Furthermore, there are types of terrorist actions with no analogues in the structure of impact factors typical of natural and technogenic disasters: for example, cyberterrorism or electromagnetic actions aimed at knocking control systems out of commission.

Global nature of terrorist threats: As a rule, the geographic distribution of sources of natural and technogenic threats is limited to regions where hazardous facilities are located or zones subject to natural hazards (river valleys for floods, seismic fault zones for earthquakes, tsunamis, and so forth). On the contrary, terrorist threats, especially those coming from international terrorist networks, are characterized by significantly more widespread distribution of the locations where a possible attack might occur.

Presence of aftereffects in the flow of terrorist actions: In contrast to natural and technogenic disasters, which may often be viewed as chains of Poisson events, after a major terrorist act the condition of the system defined as “terrorist organization—protected object—protection system” is substantially changed. On the one hand, the terrorist organization achieves its goals to one or another degree and expends a significant part of its resources, while, on the other hand, law enforcement agencies intensify the protection regime. Therefore, after a major terrorist act the situation fundamentally changes and the likelihood of a subsequent attack is significantly altered as well (generally, it is reduced). Therefore, the sequence of terrorist attacks could be described with the help of a Markov chain model. For the purpose of this model, the activities of antiterrorist forces aimed at countering the terrorist threat are understood as under control. The Markov process model makes it possible to describe the dynamics of cycles of terrorist activity.

Terrorists’ capacity for self-learning: Because terrorists are capable of analyzing the results of previous attacks and drawing conclusions from them, their experience in “successful” and “unsuccessful” attacks can have a noticeable effect on the selection of a scenario for the next attack. (Attack scenarios that have proven their effectiveness in the past have a great likelihood of being repeated by terrorists in the future, while scenarios that ended unsuccessfully will most likely be less attractive to terrorists and consequently are less likely to be repeated.) Therefore, in assessing the chances that various attack scenarios will

be realized, statistical self-learning models are more effective than traditional frequency methods.

Presence of two-way linkages between the terrorist threat and system vulnerability: One differentiating feature of a terrorist threat to a given system is the presence of two-way linkages between that threat and (1) vulnerability of the system to that threat and (2) the magnitude of expected damages if the threat is successfully realized. This characteristic of terrorist mechanisms must be examined in more detail, inasmuch as it opens up additional possibilities for reducing terrorism risks.

The formula for assessing the risk of a traditional emergency situation initiated by a natural or technogenic disaster could be presented in simplified form as follows:

$$R_c = P_{IV} \times P_{(NU/IV)} \times U_{(damage/IV \& NU)}$$

Here P_{IV} is the threat to the system, expressed as the probability of an extreme initiating action (the failure of a particular element, exceeding of allowable level for a hazard factor, extreme natural phenomenon, and so forth).

$P_{(NU/IV)}$ is the vulnerability of the system to the given initiating action, expressed as the conditional probability that damage will be inflicted if the initiating action occurs.

$U_{(damage/IV \& NU)}$ is the damage inflicted on the system if the initiating action occurs and causes damage.

Thus, for traditional natural and technogenic disasters, vulnerability is determined by a specific threat, but the consequences depend on both the type of threat and the vulnerability of the system to that type of threat. Here it should be noted that in this model there are no two-way linkages, such as the dependence of the threat on vulnerability (inasmuch as the probability of a spontaneously initiated action has no relation to system vulnerability to that action) or dependence of the threat on the consequences (for the same reason).

Therefore, the system of linkages among the risk factors for the given system in an emergency of a natural or technogenic nature is as presented in Figure 7-1A.

If the initiating action is a terrorist attack, the interactions among the various factors included in the risk assessment equation are more complex. Similar to the expression above, terrorism risk is presented as follows:

$$R_T = P_A \times P_{(NU/A)} \times U_{(damage/A \& NU)}$$

P_A is the terrorist threat to the given system, expressed as the probability that a terrorist attack of a particular type will be carried out.

$P_{(NU/A)}$ is the vulnerability of the system to a terrorist attack of the given

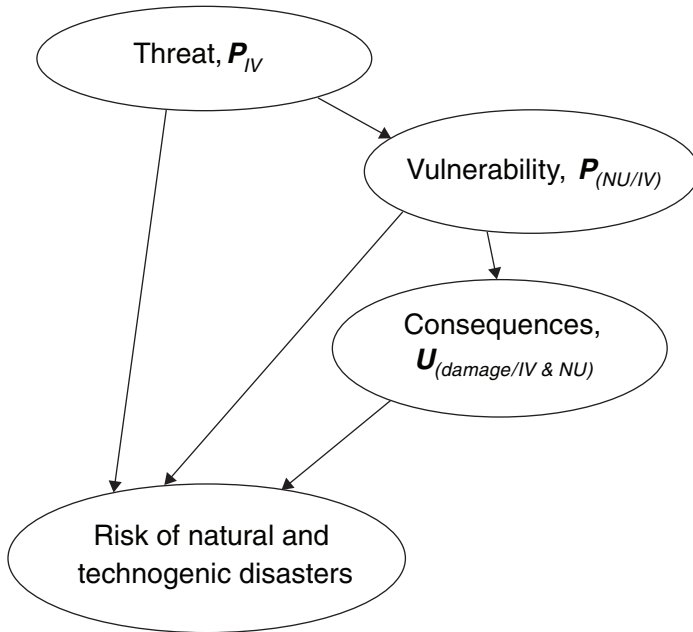


FIGURE 7-1A System of linkages among risk factors for emergency situations of a natural or technogenic nature.

type, expressed as the conditional probability that damage will be inflicted if the attack is carried out.

$U_{(damage/A \& NU)}$ is the damage inflicted on the system if the terrorist attack is carried out and causes damage.

If a terrorist action occurs, the presence of powerful two-way linkages among the risk factors should be noted (see Figure 7-1B).³ In particular, reducing the vulnerability of a given system makes it possible to reduce substantially the level of the terrorist threat it faces.

MAIN TYPES OF SCENARIOS AND IMPACT FACTORS FOR TERRORIST ACTIONS

Based on an analysis of the growing number and expanding spectrum of terrorist actions, we may conclude that scientific-technical progress presents terrorists with new opportunities for carrying out various types of terrorist acts. Successes in the development of advanced technologies and means of communication, high rates of urbanization, and the concentration of potentially hazardous

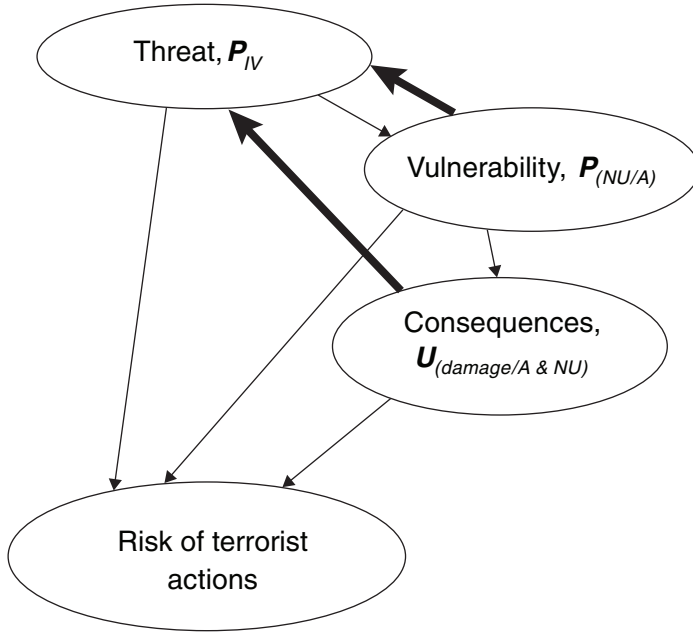


FIGURE 7-1B System of linkages among risk factors for emergency situations of a terrorist nature.

production facilities create favorable conditions for the appearance of new types of technological terrorism with especially dangerous consequences for the public and government institutions.

On the other hand, scientific-technical progress also makes it possible to protect the public and objects in the technosphere from terrorist actions. It is technical means of protection that provide the possibility of preventing terrorist acts and minimizing their consequences; that is, they make it possible to protect critically important targets, personnel, the public, and the environment.

The following section will cover the main types of scenarios for technological terrorism.

Electromagnetic Terrorism Scenarios

Modern critically important facilities (ground- and space-based communications systems, telecommunications systems, computer networks, power plants, transport control systems, nuclear industry facilities, and so forth) are vulnerable to the impact of powerful electromagnetic irradiation and penetrating high-volt-

age electrical pulses in electricity supply and grounding networks. This circumstance has led in recent years to the appearance of a real danger that scenarios for terrorist attacks based on the application of electromagnetic effects may in fact be realized.⁴

Electromagnetic terrorism scenarios entail the intentional use of electromagnetic effects against electrical and electronic systems to disrupt their normal operations. The foundations for the rise of the threat of electromagnetic terrorism were laid, on the one hand, by the sharp reduction in signal levels in electronic systems and, on the other hand, the sharp growth in achievements in creating pulse flow generators and, on their basis, electromagnetic wave emitters. The widespread introduction of electronic systems in all spheres of societal activity and the accessibility of devices used to create disruptions have given rise to the very real threat that electromagnetic terrorism scenarios may be implemented.

Electromagnetic terrorism scenarios may be divided into four main groups:

1. Injection of electrical field pulses into the electricity supply networks serving electronic devices and information systems
2. Use of super-broadband emissions to affect electronic devices and control systems
3. Creation of electromagnetic clouds to damage electric transmission lines
4. Use of electromagnetic emissions to detonate mines or other explosive devices placed for the purpose of sabotage

Cyberterrorism Scenarios

The development of computer networks and information systems based on packet commutation technology has created a new communications and information environment that is vulnerable to terrorist acts.⁵ Attacks by computer terrorists could be aimed at specific elements of the information infrastructure itself, possibly by means of computer networks, or at other targets present in one way or another in this environment. The network infrastructure as such could be of enormous value to terrorists, inasmuch as it provides a cheap and effective means of interaction and communication and serves as a source from which information may be obtained.

Thus, in addition to the multitude of positive aspects, the development of cyberspace significantly expands terrorists' arsenal of tools and capabilities. The possibilities offered by global network technologies allow terrorists to work in practically any country against targets located in any other country.

In modern industrially developed society, information technologies may be viewed by terrorists as both a target of attack and a means of attack.

Not only telecommunications and information networks but also all other components of any vitally important (critical) infrastructure whose successful

functioning depends on computer control, data processing, and digital communications could become targets for cyberattacks.

The following are highlighted as main scenarios for computer terrorism: destroying network infrastructure on a corporate, national, or transnational scale by knocking their control systems or individual subsystems out of commission; obtaining access to confidential data; changing data affecting the outcome of processes in which terrorists have an interest; or an information-related action resulting in individuals or groups behaving in accordance with terrorists' wishes.

Computer terrorism scenarios may be particularly effective if used in combination with physical actions against critically important targets. In such cases, a cyberattack is used as a factor intensifying the effect of the physical attack by countering the efforts of rapid-response services and communications and command systems, providing false output data that cause leaders and personnel to take inadequate actions, or creating panic among the public. Thus, cyberattacks increase the danger from a physical attack and exacerbate its consequences by complicating response actions and implementation of damage reduction measures.

Biological Terrorism Scenarios

The impact factors of biological terrorism can cause massive disease outbreaks and panic among people, animals, and plants.⁶ These impact factors include microorganisms and some of their products (toxins), as well as certain types of insects, both plant pests and disease vectors. In means of application, bioterrorist acts differ from other types of terrorist acts in that they can be both overt, announced, demonstrative acts as well as covert acts masked as natural outbreaks. Here it should be noted that according to current information, a significant portion of cases of bioterrorism are covert or masked in nature. Therefore, the problem of differentiating natural and artificially created disease outbreaks remains very urgent.

The effectiveness of biological terrorism scenarios is determined by the following factors:

- The world is currently witnessing the rapid development of the biological sciences, biotechnology, medicine, and pharmacology. Increasing numbers of people are employed in these fields and have the necessary knowledge and qualifications to develop and manufacture bioweapons. There is a growing number of laboratories and biological and pharmaceutical plants that have the necessary conditions for producing biological weapons.
- Manufacturing biological weapons is relatively simple and inexpensive. With the appropriate pathogenic virus or microorganism strain, a pathogen can be produced in rather large quantities without particular problems in any laboratory

with the capacity to support work under sterile conditions. Such conditions are relatively easy to create even at home.

- The problem of the pathogenic bacterial or viral strain is that although it is one of the most complex problems bioterrorists face, it is also solvable. Bioterrorists can obtain the pathogen illegally through a laboratory or production facility where these microorganisms or viruses are studied or where related vaccines or diagnostic test kits are produced. Bioterrorists can then pass the pathogenic viral or microbial strain along to another terrorist group.

- Bioweapons are effective in very small doses. The ease of concealing bioweapons, the covert manner in which they can be used, the lack of external manifestations at the moment of release, and the relative ease with which they can be produced make it very unlikely that their use will be detected and prevented.

- Biological weapons make it possible to carry out both individual terrorist acts and massive strikes against people, animals, and plants.

- At present, there are practically no technologies for protecting against bioweapons or detecting and identifying a pathogenic microorganism or toxin before it begins to take effect. Therefore, a case of bioterrorism can be discovered only after the outbreak begins and is identified, which can take a fairly long time after large numbers of people, animals, or plants have already been infected.

Thus, the relative ease of producing biological weapons, the practical invulnerability of the perpetrators, and the possibility of damages on a huge scale make biological attack scenarios attractive to terrorists.

Chemical Terrorism Scenarios

Dangerous chemicals are found everywhere in modern industrial society and, consequently, may be accessible to terrorists.⁷ The following four attack scenarios related to chemical terrorism may be highlighted:

1. Dispersal of a military chemical substance for nonmilitary purposes
2. Sabotage at a chemical plant or storage facility (including rail tank cars) where there are toxic chemicals stored in gaseous, liquid, or solid form that can react with air or water to produce toxic gases or evaporate into the atmosphere
3. Contamination of natural water sources or drinking water reservoirs with toxic substances
4. Intentional use of chemical substances to kill individual people

Terrorists may realize their intentions of acquiring chemical weapons in two ways: (1) by buying (stealing) them from existing national stockpiles or (2) by producing them at their own underground enterprises. Inasmuch as synthesizing military chemical substances requires overcoming complex technical barriers and entails great risk, it is more likely that terrorists will acquire highly toxic indus-

trial chemicals. Although such substances are hundreds of times less lethal than paralyzing nerve gas, they nevertheless can cause significant losses if used in a closed space or in the open air under favorable atmospheric conditions.

Military chemical substances are poisonous, artificially created gases, liquids, or powders that upon entering the body through the lungs or skin cause disability or death among people and animals. Although many military chemical substances are liquids, they can be put into the form of an aerosol (fine mist of tiny droplets) and then evaporate into the atmosphere as a result of the detonation of a shell. Most chemical substances fall into one of five broad categories: (1) skin-blistering agents, (2) paralyzing nerve agents, (3) asphyxiating gases, (4) bleeding agents, and (5) disabling agents. Besides the various psychological effects that they produce, chemical weapons also differ from one another in their resistance to destruction, volatility, and evaporation rate. Unstable substances are dispersed in the air for several hours and mainly present a threat if they are inhaled, while persistent substances remain dangerous for a month if they are scattered on the soil, vegetation, or objects and, as a rule, represent a hazard if they make contact with skin.

Chemical substances with skin-blistering effects, such as yperite (mustard gas) or lewisite, are liquids that cause chemical burns.

Nerve-paralyzing substances like sarin and VX are the most powerful chemical poisons known. They disrupt the human nervous system and kill their victims within a few minutes. Given the extreme danger associated with handling or storing nerve-paralyzing agents, terrorists might attempt to develop a binary weapon that would be safer to produce, store, and transport. A binary system presumes the separate storage of two relatively nontoxic ingredients and their mixture immediately before use to create a lethal substance. Sarin, for example, could be produced in a binary system through the chemical reaction of isopropanol with methylphosphoryldifluoride (DF). However, synthesizing DF is complicated and difficult. Furthermore, terrorists would have to either mix the components manually before use, which is an extremely dangerous operation, or try to develop a remote-controlled device to handle the mixing and dispersal, which in turn would require a high degree of technical skill.

A very likely terrorist attack scenario would be a case of sabotage at an industrial enterprise that manufactures, processes, or stores highly toxic chemicals, leading to their emission or discharge with subsequent impacts on nearby populated areas. A dangerous chemical could be intentionally discharged by destroying a chemical container with the help of a conventional explosive device or by sabotaging the manufacturing process at the facility, leading to an emergency situation. Terrorists could also set off an improvised explosive device to blow a hole in a rail tank car being used to transport a dangerous chemical.

Historical experience shows that most well-known chemical terrorism attacks were committed using household and industrial chemicals. Although these substances are less toxic than military poisonous substances, their consequences

may be catastrophic. Therefore, in addition to countering attack scenarios using military poisonous substances, it is recommended that significant attention be devoted to attack scenarios involving sabotage at facilities producing, using, or transporting hazardous chemicals.

Radiation Terrorism Scenarios

Scenarios for terrorist acts using radiation sources may be divided into three groups: (1) detonation of a nuclear explosive device, (2) sabotage at nuclear facilities, and (3) radiological terrorism.⁸

Detonation of a Nuclear Device

Scenarios in this group relate to a more dangerous type of terrorism from the standpoint of the scope of the consequences. Such scenarios entail the theft of a nuclear explosive device from a storage arsenal or the creation of a homemade nuclear bomb using highly enriched uranium or plutonium. Realization of these scenarios is complicated by the circumstances that the key components necessary for manufacturing nuclear weapons systems—that is, fissionable materials (plutonium or highly enriched uranium)—are difficult to obtain, and the capabilities and equipment needed to produce them also have their specific characteristics. However, although nuclear weapons systems are complex technical devices, it is impossible to rule out the possibility that a well-trained terrorist organization could be capable of manufacturing a primitive nuclear device with a yield up to the tens of kilotons.

The most difficult part of manufacturing such a nuclear device is acquiring the necessary quantity (on the order of several kilograms) of highly enriched uranium or plutonium. Therefore, preventing nuclear weapons and weapons materials from falling into the hands of terrorists is a top priority.

Sabotage at Nuclear Facilities

Scenarios in this nuclear terrorism category entail setting off an explosion at a facility such as a nuclear power plant, research reactor, spent fuel reprocessing plant, radioactive waste repository, or similar site.

Numerous nuclear facilities present very attractive targets for terrorists. The potential destruction and damage that could be caused by a terrorist act at a nuclear reactor depend on the design characteristics of the given reactor and the protective measures in place, which in turn vary widely at the different types of facilities. According to data from the International Atomic Energy Agency (IAEA), 438 nuclear reactors are operating in the world today.

Radiological Terrorism

This type of terrorism involves detonating a conventional explosive device containing radioactive isotopes with the aim of subsequently dispersing them over a significant area. This category also includes attack scenarios in which radioactive substances are dissolved in water sources. This category of radiation terrorism scenarios is not as powerful in impact as the first category, but is much more likely to be used by terrorists. So-called radiological dispersal devices could be manufactured by packing radioactive materials together with chemical explosives and then detonating the device.

Scenarios for Terrorist Attacks Using Explosives

Because the goal of any terrorist act is to create maximum resonance in society with minimal costs and minimal risk, the use of explosives for terrorist purposes has become widespread. Potential targets of terrorist attacks could include critically important facilities of undoubted interest from the standpoint of inflicting damage and creating significant societal impact.⁹

From the standpoint of the likelihood of technological terrorist attacks, such acts at enterprises using large volumes of flammable substances in their technological processes (gas stations, compressed gas facilities, oil refineries, chemical plants, and so forth) represent a serious potential danger. If explosives are detonated at enterprises using explosive or flammable substances, the following attack scenario is possible: (a) release and dispersal of large volumes of flammable substances, (b) their mixture with air in the necessary proportions and formation of an explosive cloud, and (c) its subsequent explosion. The detonation of explosive clouds over a city could lead to significant destruction and fatalities. Facilities using poisonous substances must be considered as a separate category. Significant destruction at such sites is capable of releasing into the atmosphere a large volume of poisonous substances circulating in the facility's systems, which could contaminate large areas of the city. A separate target for potential technological attacks by terrorists could be a city's natural gas system (gas distribution points, stations, pipelines, underground facilities, and even individual apartments with gas appliances).

Explosive transformation is generally classified in one of two categories deflagration and detonation which are differentiated by the dynamics of the explosive load. The main impact factors from a detonation explosion are an atmospheric blast wave characterized by excess pressure and the force of the compression wave and a fireball created by extremely hot combustion products. The main impact factors from a deflagration explosion are (1) a compression wave characterized by maximal excess pressure, (2) dynamic pressure, (3) wind effects that can substantially exceed centrifugal load, (4) and a fireball of extremely hot combustion products.

MODELING TERRORIST THREATS AND TERRORIST ATTACK SCENARIOS

As noted previously, the distinguishing characteristics of technological terrorism scenarios and impact factors are shaped by the capacity of terrorists for deliberately choosing the means, place, and time for the attack. This choice is based on a rational assessment of (1) the vulnerability of the given target to various attack scenarios and (2) the magnitude of the damages expected if the various attack scenarios are carried out. The decisions made by the terrorists are based on the minimax principle, which consists of a striving to inflict maximum damage on society while expending the minimum resources and with minimal risk that the organization will be detected and eliminated (that is, a striving to ensure maximum effectiveness for the attack). Here, terrorists are capable of reacting to the actions of antiterrorist forces, drawing lessons from the experience of previous attacks, and using them to correct their actions. Additional difficulties that must be faced in evaluating the likelihood that various terrorist attack scenarios will be carried out are associated with the value system of terrorists (that is, their usefulness function) differing notably from the traditional value system. Their system of motivating principles often is not fully comprehensible even to specialists.

Furthermore, the following characteristics are typical of the issues faced in evaluating terrorist attack threats (impact factors) and scenarios:

- High level of uncertainty due to lack of knowledge of terrorists' intentions, intellectual potential, and organizational-technical resources, the goals they are pursuing, and the value system by which they are guided
 - Fragmentary and (often) secret nature of data of various types obtained from various sources, such as statistical information, expert assessments, and operational information obtained from intelligence services
 - Dynamic nature of terrorist risks

The mathematical model being developed for evaluating various terrorist attack scenarios for a given target must meet the following requirements:

- The model must facilitate assessments and decision making for situations involving a very high level of uncertainty.
- The model must be multidimensional; that is, it must consider a situation from the standpoint of both terrorists and antiterrorist forces. It must provide for a description of the dynamic interaction of these two sides, each of which is guided by its own strategy and is capable of reacting to its opponent's actions. Furthermore, the model must make it possible to take into account terrorists' capacity for selecting the attack scenario that ensures maximum attack effectiveness. That is, it must include the two-way linkages between the vulnerability of the system to

the given attack scenario (and the expected damage) and the likelihood that this attack scenario will be selected by terrorists.¹⁰

- The part of the model that characterizes terrorists' situational analysis and decision making (part 1 of the model) must assess terrorists' goals, value system, resources, and intellectual and organizational-technical potential; identify basic scenarios for terrorist attacks against a given target; and must assess the probability that various terrorist attack scenarios will be carried out based on their usefulness function, by which (in the opinion of antiterrorist analysts) terrorists must be guided.

- In addition to providing an assessment of vulnerability of the given target and the effectiveness of its protection systems, the blocks of the model that describe the situation from the antiterrorist standpoint must also use results obtained on the basis of analysis of the terrorist part of the model (particularly the likelihood of various attack scenarios being realized from the viewpoint of the terrorists) to determine the most effective measures for countering the terrorist threat. In this regard, the possibility of interaction among the various forces countering the terrorist threat and of exchanges of information among them must be taken into account.

- The model must be dynamic; that is, it must make it possible to describe the change of parameters of the system (target), the external environment, and the spectrum and intensity of terrorist threats.

Given these requirements, it makes sense to bring to bear the principles of game theory¹¹ and Bayesian networks,¹² which make it possible to (1) take into account the independent actions and rational behavioral strategies of terrorist and antiterrorist forces; (2) assess situations characterized by high levels of uncertainty; and (3) account for information obtained from various sources (including information received periodically on the status of particular variable models), thus making it possible to obtain detailed inductive assessments of the likely accuracy of the predictions of other variable models.

Scientific methodological aspects and applied developments have become the focus of joint analysis within the framework of a program for countering technological terrorism being carried out jointly by the Russian Academy of Sciences and the U.S. National Academy of Sciences¹³ and under the Science for Peace Program of the North Atlantic Treaty Organization.¹⁴

Figure 7-2 presents a three-sided model that facilitates assessment of terrorist attack scenarios and counteractions by antiterrorist forces. The model consists of three graphs. Graph 1 is a diagram of influence describing the situation involved in making decisions to select an attack scenario from the standpoint of a terrorist organization. This diagram is compiled by analysts at the security service of a target facility, who, in their attempt to consider things from the terrorists' position (playing the role of the enemy), strive to assign values for expected usefulness for the terrorists if various attack scenarios were to be carried out. The values arrived

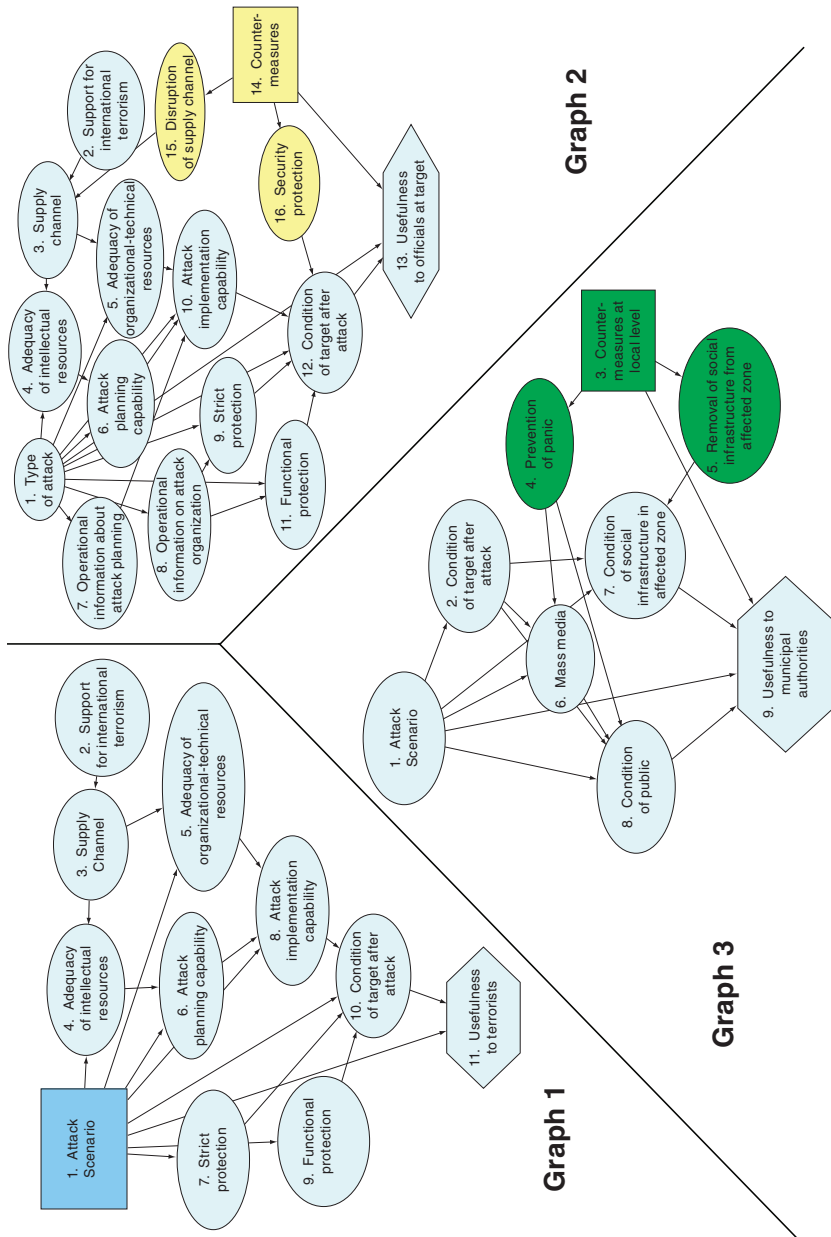


FIGURE 7-2 Three-sided terrorism risk assessment model.

at then make it possible to assess the probability of the various attack scenarios being realized. These probabilities are used in constructing graphs 2 and 3, which characterize the corresponding process of making decisions to select measures to counter the terrorist threat at the level of the security service of the given facility (Graph 2) and at the level of the municipal authorities in the area where the facility is located (Graph 3). It should be kept in mind that facility officials and the municipal authorities can exchange information and coordinate their efforts; that is, they are allies in the game.

The similarities and differences between the graphs show that they describe the same question but from different positions. For instance, the differences between the graphs reflect the varying level of uncertainty regarding the condition of specific elements (the condition of the same element—for example, the resources of the terrorist organization could be known for certain by the terrorists but viewed by antiterrorist forces as a random value). Assessments of the probability links between task variables (that is, the tables of conditional probabilities for the three graphs) also differ accordingly. In addition, some task parameters may not be considered at all by one side but, at the same time, could be very important to the other. Fundamental differences are also noted in the usefulness elements of each graph, inasmuch as the usefulness functions for terrorists, facility officials, and the municipal authorities may take completely different factors into account. Terrorists, for example, may be oriented primarily toward infliction of the initial blow and on the expenditures necessary for carrying out the attack, while for facility officials the usefulness function must also include secondary damage and the cost of implementing various protective measures. The usefulness function for the municipal authorities must first take into account the damage inflicted on the public and the local infrastructure in areas near the target facility.

NOTES

1. Frolov, K., and G. Baecher. 2006. *Protection of the Civilian Infrastructure from Acts of Terrorism*. Dordrecht, The Netherlands: Springer, 252 pp.

Pate-Cornell, E. 2002. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Operations Research* 7(4):5-20.

Woo, G. 2004. Quantitative terrorism risk assessment. Available online at www.rms.com/NewsPress/Quantitative_Terrorism_Risk_Assessment.pdf. Accessed April 11, 2008.

2. *Technogenic* is used to refer to phenomena arising as a result of the development or deployment of technology.

3. Makhutov, N. A., and D. O. Reznikov. 2007. Use of Bayesian networks to assess terrorist risks and select an optimal strategy for countering the terrorist threat. *Problems of Security and Extreme Situations* 5:43-63.

Pate-Cornell. Probabilistic modeling of terrorist threats.

4. Fortov, V. E. 2004. Study of electromagnetic impacts in terrorist and antiterrorist actions. Pp. 228-238 in *Proceedings of a Scientific-Practical Conference*. Moscow: Kombitell.

5. Barsukov, V. 2000. Protecting computer systems from powerful destructive effects. *Jet Info Information Bulletin* 2(81):8-17. Available online at www.jetinfo.ru/2000 (in Russian).

Vasenin, V. A., and A. V. Galatenko. 2002. Computer terrorism and Internet security problems. Pp. 211-225 in *High-Impact Terrorism: Proceedings of a Russian-American Workshop*. Kirov, Russia: Vyatka. [Pp. 183-197 in the original English version by the same title, published in 2002, Washington, D.C.: The National Academies Press.].

Branscomb, L. 2003. Cyberattacks as an amplifier in terrorist strategy. Pp. 93-96 in *Terrorism: Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings*. Washington, D.C.: The National Academies Press.

6. Morenkov, O. S. 2002. Bioterrorism: A view from the side. Pp. 131-141 in *High-Impact Terrorism: Proceedings of a Russian-American Workshop*. Kirov, Russia: Vyatka. [Pp. 106-113 in the original English version by the same title, published in 2002, Washington, D.C.: The National Academies Press.].

McGeorge, J. 2001. An analysis of 404 nonmilitary incidents involving either chemical or biological agents. P. 53 in *Abstract Book of the World Congress on Chemical and Biological Terrorism*, Dubrovnik, Croatia, April 22-27, 2001.

7. Ibid.

8. Aratyunyan, R. V., V. Belikov, et al. 1999. Models for the spread of radioactive contamination in the environment. *RAS Power Engineering News* 1:61-96.

Hecker, S. 2002. Nuclear terrorism. Pp. 176-184 in *High-Impact Terrorism: Proceedings of a Russian-American Workshop*. Kirov, Russia: Vyatka. [Pp. 149-155 in the original English version by the same title, published in 2002, Washington, D.C.: The National Academies Press.].

9. Komarov, A. A. 2004. Questions of protecting the urban infrastructure and the public from explosive technological terrorism and catastrophic explosions. Pp. 79-89 in *Proceedings of a Scientific-Practical Conference*. Moscow: Kombitell.

Simmons, R. 2002. Terrorism: Explosives threat. Pp. 199-211 in *High-Impact Terrorism: Proceedings of a Russian-American Workshop*. Kirov, Russia: Vyatka. [Pp. 171-179 in the original English version by the same title, published in 2002, Washington, D.C.: The National Academies Press.].

10. The use of two-sided models describing the terrorist and antiterrorist sides of a conflict is described in detail in Pate-Cornell, Probabilistic modeling of terrorist threats.

11. Hausken, K. 2002. Probabilistic risk analysis and game theory. *Risk Analysis* 22(1):17-27. McCain, R. Game theory: An introductory sketch. Available online at william-king.www.drexel.edu/top/eco/game/nash.html.

Sandler, T., and D. Arce. 2003. Terrorism and game theory. *Simulation and Gaming* 34(3).

12. Terekhov, S. A. 2003. Introduction to Bayesian networks. Scientific session of the Moscow Engineering-Physics Institute, Fifth All-Russian Scientific Practical Conference, Moscow; Jensen, F. V. *An Introduction to Bayesian Networks*. 1996. New York: Springer-Verlag.

13. National Research Council Committee on Counterterrorism Challenges for Russia and the United States. 2004. *Terrorism: Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings*. Washington, D.C.: The National Academies Press.

14. Frolov and Baecher. Protection of the Civilian Infrastructure.

Additional background materials not specifically cited:

Petrov, V. P., D. O. Reznikov, V. I. Kuksova, and Ye. F. Dubinin. 2007. Terrorist risk assessment and decision-making on the expediency of building a protection system against terrorist actions. Pp. 89-105 in *Problems of Security and Emergency Situations*, vol. 1.

Tucker, J. 2002. Chemical terrorism: Assessing threats and responses. Pp. 141-165 in *High-Impact Terrorism: Proceedings of a Russian-American Workshop*. Kirov, Russia: Vyatka. [Pp. 117-133 in the original English version by the same title, published in 2002, Washington, D.C.: National Academies Press.].

Frolov, K. V., and N. A. Makhutov. 2004. Technological terrorism and methods of countering terrorist threats. Pp. 228-238 in *Proceedings of a Scientific-Practical Conference*. Moscow: Kombitell.

Emerging Viral Infections in the Asian Part of Russia

Sergei V. Netesov, Federal State Research Institution—State Research Center of Virology and Biotechnology Vector and Novosibirsk State University, and Natalya A. Markovich, Federal State Research Institution—State Research Center of Virology and Biotechnology Vector

The so-called emerging infections are primarily the result of increased human activities such as international and domestic trade, tourism, industrialization and its consequences, and, to a lesser extent, climate change, which are detailed in this paper. The stages of emergence and spread of highly pathogenic subtype H5 avian influenza virus over the territory of Russia in 2005-2007 are considered, as well as the corresponding measures of its control. It is now well known that the mortality rate resulting from emerging infections is considerably higher than that caused by bioterrorism. At the same time, bioterrorists may use emerging infectious agents for bioterrorist acts. Therefore, emerging and reemerging infectious diseases are of substantial interest in the biosecurity community because some of these agents can be used for intentional attacks. In addition, natural outbreaks can help highlight vulnerabilities and gaps in public health or agricultural response capabilities. Therefore, it makes sense to intensify development of measures to control emerging infections, which will also enhance the struggle against bioterrorism.

Since the 1980s, physicians and specialists have encountered the emergence of new infectious diseases—emerging infections—with ever-increasing frequency. The new emerging infections appear once every 2 or 3 years. Each infection has its own specific features; therefore, each requires special attention from scientists and public health care practitioners.

Seven main reasons underlie the emergence of new infections:

1. Transfer of infections from one region of the world to another by migratory birds
2. Human colonization of new territories inhabited by previously unknown animals or insects
3. Industrial breeding of animals, particularly new animal species, or introduction of new species of pets
4. Introduction of animals to new territories where they have not previously lived
5. Global warming and the subsequent invasion of new animal and insect species
6. Creation of new conditions for reproduction of animals and insects as a consequence of human activities
7. Adoption of new technologies, which not only improves human life but also creates new conditions for the reproduction of pathogenic microorganisms

Let us consider each of these issues individually.

TRANSFER OF INFECTIONS BY MIGRATORY BIRDS (EXAMPLE: H5N1 INFLUENZA VIRUS)

The map in Figure 10-1 illustrates the epizootic caused by avian influenza virus in western Siberia in the summer of 2005. The first mass mortality event, initially affecting wild birds and subsequently domesticated species, was recorded by the Federal Agency for Veterinary and Phytosanitary Surveillance (Rosselkhoz nadzor) in the village of Suzdalka, Dovolnoye Region, Novosibirsk Oblast (Shestopalov et al., 2006; Evseenko et al., 2006; and Lipatov et al., 2007). After the regional Rosselkhoz nadzor office received the report from this village about the deaths of wild birds, it notified other regions of Novosibirsk Oblast and neighboring jurisdictions. Veterinarians began detecting disease in wild birds and later in domesticated birds at many sites in western Siberia and reported their findings to the local Rosselkhoz nadzor offices. In particular, analogous epizootics were recorded in July-August 2005 in wild birds and subsequently in domesticated species in Altai Krai and Novosibirsk, Tomsk, Kemerovo, Omsk, and Kurgan oblasts, as well as in Pavlodar Oblast in Kazakhstan (Lipatov et al., 2007).

Note that the threat to domesticated birds in individual and commercial farms was very serious, as these regions are known for mass poultry breeding on both private and industrial scales. Physical security is practically absent on individual farms but is sufficient on most commercial farms, which are equipped with ventilation tubes and doors as well as mesh-covered windows to prevent wild and domestic birds from mixing. In addition, at commercial farms grain is heat treated before feeding, and personnel and their clothing are disinfected at build-

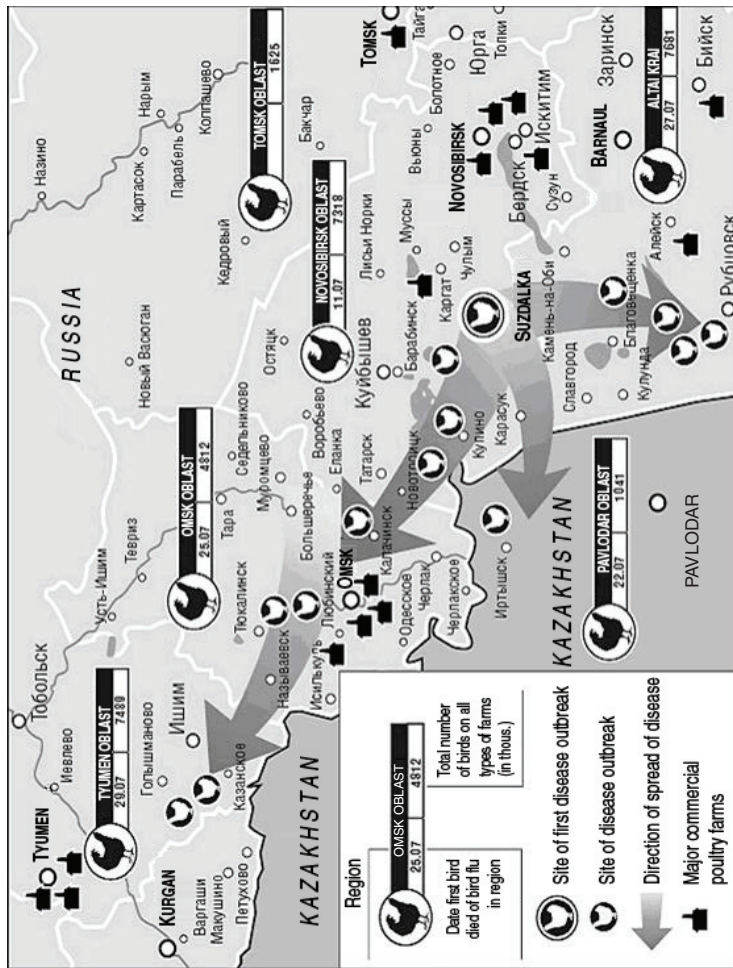


FIGURE 10-1 Map of epizootics caused by H5N1-subtype avian influenza virus in Russia in summer 2005.

NOTE: In the black boxes, the names of regions, amount of both individual and industrial domesticated birds, and dates of first notification made by local (county) Rosselkhoznadzor officers are shown.

ing entrances and exits. The poultry stock in individual and commercial farms in Novosibirsk Oblast amounts to approximately 7.3 million; in Omsk Oblast, 4.8 million; in Tyumen Oblast, almost 7.5 million; and in Altai Krai, nearly 7.7 million birds. One of the most likely causes of mortality among domesticated birds was avian influenza virus, which, as is known from the events of 2003-2004 in Southeast Asia, represents a tremendous threat for poultry farming. Thus, it was clear that the most serious measures were required to control this disease, even not taking into account the potential threat of human morbidity and mortality.

The sequence of events for diagnosis of the disease and study of the properties of avian influenza virus strains in Russia in July 2006 was as follows:

- July 11, 2006: A gamekeeper from the village of Suzdalka and a veterinary officer from Dovolnoye Region reported to the regional office of Rosselkhoz nadzor about a mass mortality of wild birds on Suzdalka Lake.
- July 15, 2006: The first recording of the mass mortality event among domesticated birds in the village of Suzdalka, Novosibirsk Oblast, was made; the first team from the State Research Center of Virology and Biotechnology Vector was sent to Suzdalka.
- July 17-18, 2006: A sampling of organs and feces from domesticated birds was taken by the Vector team, and the samples were delivered to Vector; assaying of samples began.
- July 20, 2006: The first results of analysis (identification of the pathogen as the H5 subtype of the avian influenza virus) were reported to the governor of Novosibirsk Oblast and the regional and central offices of the Federal Monitoring Service for Consumers' Rights and Welfare (Rospotrebnadzor).
- July 22, 2006: The results of further analysis (genotype H5N1 and high pathogenicity for chicks) were reported to the governor and offices of Rosselkhoz nadzor and Rospotrebnadzor.
- July 24, 2006: Complete nucleotide sequences of hemagglutinin (HA) and neuraminidase (NA) genes of the virus were determined and their phylogenetic similarity to influenza virus strains isolated in China in April-May 2005 from birds on Qinghai Lake was demonstrated; data on potential pathogenicity for humans were obtained based on molecular genetic characteristics (Evseenko et al., 2006).
- July 24, 2006: A specialized commission was organized on order of the governor of Novosibirsk Oblast for control of the epizootic (control measures included exterminating infected birds, disseminating information about the epizootic to the public, and preventing the spread of the epizootic).

The five main properties of the Suzdalka influenza virus strain isolated at Vector are listed below (these data were reported on July 24, 2006, to the governor of Novosibirsk Oblast and territorial and central offices of Rospotrebnadzor):

1. According to serological and genetic data, the isolated strain was of the H5N1 subtype.
2. The hemagglutinin cleavage site of this strain contained six positively charged amino acids, thus indicating its potential pathogenicity for humans.
3. Analysis of the nucleotide sequence of the M2 gene of this strain demonstrated amantadine sensitivity.
4. Phylogenetic analysis of the HA and NA gene sequences demonstrated that this strain was most similar to strains isolated in May 2005 from dead wild migratory birds on Qinghai Lake in central China.
5. Analysis of intravenous pathogenicity in chicks demonstrated that this strain displayed the highest pathogenicity index, IVPI = 3, meaning one-half of the infected chicks died during the first 24 hours after infection (Evseenko et al., 2006; L'vov et al., 2006; and Lipatov et al., 2007).

During July 2005, this virus was detected in the majority of oblasts in the southern part of western Siberia and in several oblasts of Kazakhstan, having caused extensive epizootics with mass mortality of wild fowl and domesticated birds in individual open-type farms. Analogous outbreaks were recorded during 2005 in northern Mongolia and northeastern China, that is, in the particular territories crossed by migratory flyways from China to Kazakhstan and Russia. The epizootics in Novosibirsk Oblast and other oblasts of the southern part of western Siberia were virtually stopped by August 2005 by exterminating the sick birds and their avian contacts in the villages and subsequently disinfecting the farmsteads and preventing domesticated birds from coming into contact with wild aquatic birds.

It was clear that this outbreak could be repeated in the fall, as the migratory birds from northern Siberia would cross southern Siberia on their way to wintering sites. Therefore, to prepare an avian influenza forecast for the fall of 2006, the team of experts from Vector, the Institute of Animal Systematics and Ecology, Siberian Branch of the Russian Academy of Sciences, and the regional Rosselkhoz nadzor office constructed a map of autumn flyways for the migratory birds of western Siberia (see Figure 10-2). Based on this map, it was assumed that the H5N1-subtype influenza virus could be brought from the northern part of western Siberia back to southern Siberia as well as to China and Mongolia. The virus could also be transferred to Kazakhstan, Uzbekistan, Turkmenistan, and the European part of Russia, and from these regions to western European countries. In fact, it actually reached eastern and some central European countries. In Turkey and Romania it led to considerable decreases in or even bans of poultry exports, which caused substantial financial losses.

This was in fact what happened. Influenza outbreaks in the fall of 2005 were recorded in Tula, Moscow, Chelyabinsk, Tambov, Novosibirsk, Omsk, Kurgan, and Tyumen oblasts and in Altai Krai. In addition, in Kurgan Oblast the virus first appeared in a large commercial poultry farm. Consequently, the entire stock

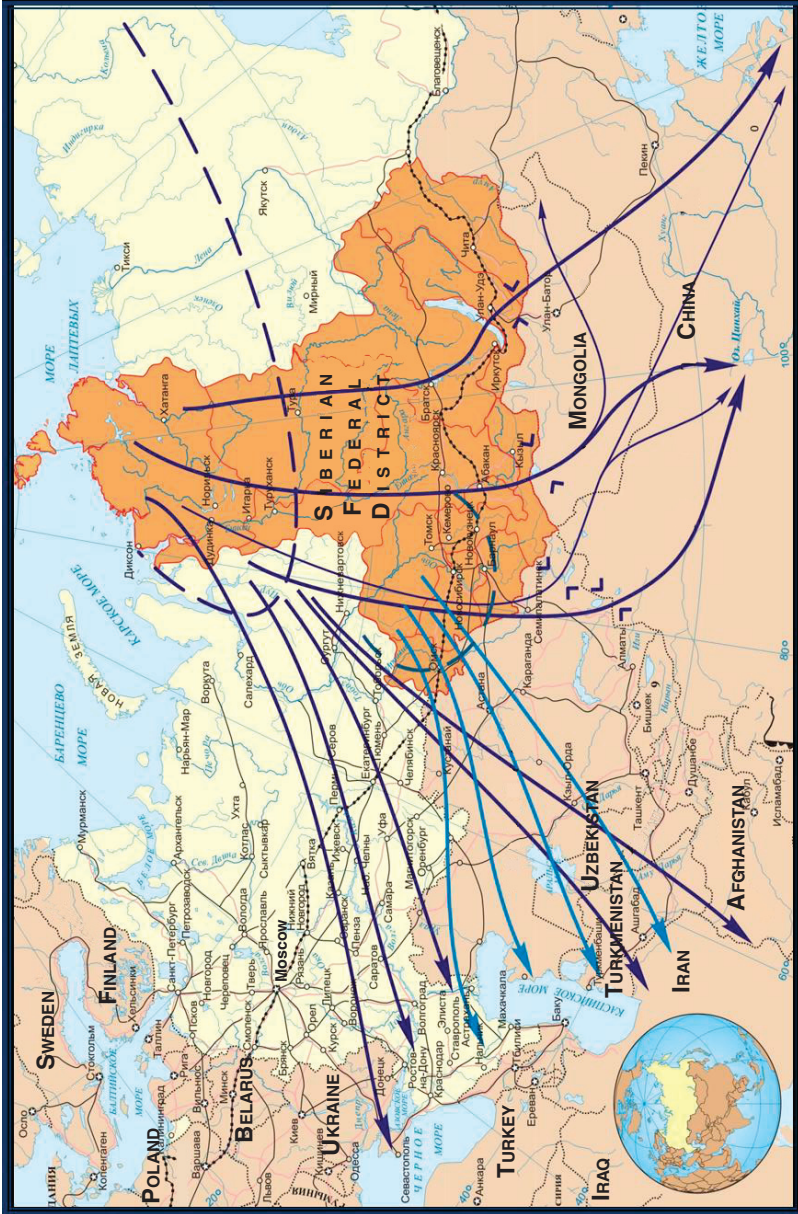


FIGURE 10-2 Flyways of the fall migration of migratory birds crossing the territory of Siberian Federal District.

of 450,000 hens and chicks was exterminated. This virus was also transferred to European countries: Epizootics occurred in Croatia, Romania, Ukraine, and Turkey. Subsequent sequencing with phylogenetic analysis demonstrated that all the isolates were closest to viruses of the Qinghai group, similar to the viruses from Novosibirsk Oblast (Onishchenko et al., 2006; Onishchenko et al., 2006; Onishchenko et al., 2007).

Later, in the winter of 2005-2006, epizootics caused by similar influenza virus strains were observed in Crimea and Ukraine. As it has been shown later by molecular biological investigations, the virus in Ukraine was practically the same as it was in Siberia in the summer and fall of 2005 (see Onishchenko et al., 2007). In February 2006, mortality of wild birds was recorded in Azerbaijan; however, sick and dead birds were secretly picked up and eaten by local residents. As a result, eight human cases with five lethal outcomes were recorded there. The infection was most likely caused when people inhaled aerosolized fecal matter from sick birds, which contained the virus, as they were plucking and cutting bird carcasses.

In March 2006, cases of avian influenza were recorded in both wild and domesticated birds in open-type individual and collective farms in Dagestan and Krasnodar Krai, where more than 1 million birds were killed to stop the spread of the epizootic. Influenza outbreaks among wild birds were recorded in March in Georgia and in western Kazakhstan (the city of Aktau). In April-May, new epizootics were recorded in China, in the Qinghai Lake region and Tibet Province. In May, outbreaks were recorded in western and central Mongolia on Uvs-Nuur Lake. This lake borders Russia; therefore, the outbreaks took place in Russia as well, on the northern coast of the lake. In addition, outbreaks among wild birds and, in some cases, among domesticated birds were recorded in Novosibirsk and Omsk oblasts and Altai Krai in May-June. Following these outbreaks, local offices of Rosselkhoznadzor immediately banned transportation of poultry products to other regions of Russia and abroad. Note that in the spring of 2006, almost all the stock on individual poultry farms in western Siberia was inoculated with inactivated vaccine based on the H5N1-subtype influenza virus, and an epizootic in Novosibirsk Oblast was recorded only in the village of Reshety, Dovolnoye Region, where the inhabitants refused to vaccinate their domestic fowl. Thus, their unintentional experiment demonstrated that the veterinary vaccine used was actually effective (personal communication of Rosselkhoznadzor official).

Later, in June 2006, epizootics were also recorded in Odessa, Kherson, and Sumy oblasts (Ukraine). During the summer, outbreaks occurred in several oblasts of southern Russia, mainly among wild birds but also sometimes on individual farms. All the above data about avian influenza outbreaks in Russia and in neighboring countries have been extracted from specialized Russian Internet sites (www.rospotrebnadzor.ru and fsvps.ru/fsvps/links/structureLinks.html?_language=ru), nonspecialized Russian Web sites (www.regnum.ru and

www.rbc.ru), and the Web site of the World Organization for Animal Health (www.oie.int).

During the spring and summer of 2006, disease outbreaks caused by the H5N1-subtype avian influenza virus were recorded in Ukraine (Odessa, Kher-son, and Sumy oblasts). That summer, additional outbreaks were noted in European Russia (Kabardino-Balkaria; Chechen Republic; the republics of Adygeya, Dagestan, and Kalmykia; Stavropol and Krasnodar krajs; and Astrakhan, Volgograd, and Rostov oblasts, where mortality was observed both among wild and domesticated birds on individual farms).

It is evident from the phylogenetic tree that we constructed (see Figure 10-3) that the H5 virus strains isolated in 2006 were somewhat different from the strains of 2005 (Lipatov et al., 2007). In addition, the isolates recovered in western Sibe-

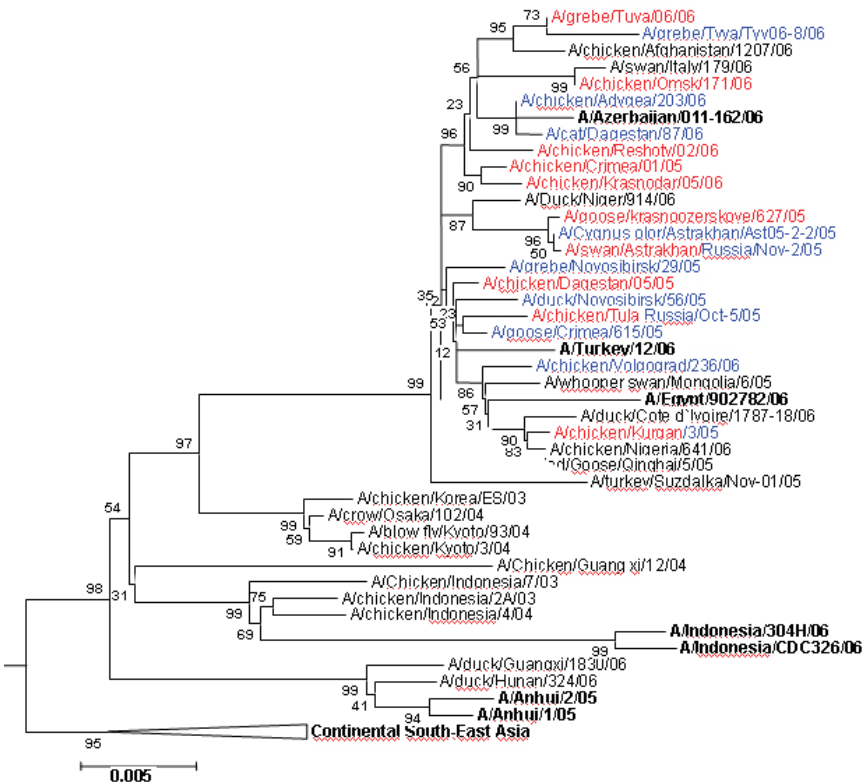


FIGURE 10-3 Phylogenetic tree constructed based on sequences of the HA gene of H5N1-subtype avian influenza virus isolates recovered during 2005-2006 compared with data from other centers.

ria in 2005 were heterogeneous and differed not only in their nucleotide sequences but also in their biological properties. For example, the strains isolated in the village of Krasnoozerskoye and in Dovolnoye Region in Novosibirsk Oblast—only 200 kilometers apart—differ fundamentally in their pathogenicity for mice: 1,000-fold in the infection dose, 10,000-fold in LD₅₀ (dose lethal to 50 percent of subjects), and in the virus titers in the lungs, brain, and kidneys of the infected mice (see Table 10-1). Thus, strains pathogenic not only for birds but also for mammals were already circulating in Novosibirsk Oblast in the summer of 2005. Consequently, an avian influenza virus strain pathogenic for humans probably could have been circulating in Siberia at that time; perhaps the population of western Siberia was just lucky to avoid human influenza cases caused by the H5-subtype influenza virus. Note that all severe respiratory disease cases at least in Novosibirsk Oblast and in neighboring regions of western Siberia in 2005-2006 were thoroughly monitored. All samples from such human cases were examined for markers of H5-subtype influenza virus both at local laboratories and, in case of an even slightly positive result, at Vector Center; however, no human cases of H5 avian influenza were detected (Evseenko et al., 2006).

In 2006 the following anti-epidemic measures were introduced in western Siberia and all of Russia to control epizootics of influenza virus in birds and to prevent outbreaks of this disease in humans:

- Information was provided about the need to avoid close contact with sick and dead birds (the public, especially in villages, was alerted not only through the media but also with leaflets).
- Acute respiratory disease cases among the rural population were thoroughly monitored, including analysis of suspected cases by real-time polymerase chain reaction (PCR) at Vector and other laboratories in the region. The PCR test was practically identical to the World Health Organization (WHO) test. The Russian PCR test kit was produced by InterLabService, Inc. in Moscow.
- The rural population and high-risk population cohorts in regions with recorded epizootics caused by H5N1 avian influenza virus in birds were vaccinated against seasonal influenza. This vaccination was recommended by the World Health Organization and was conducted in the spring and fall using Russian-manufactured vaccine.
- Domesticated birds on both individual and commercial farms where a mass mortality was recorded and the pathogenic influenza virus was found were exterminated by specially trained teams from the Ministry for Emergency Situations and veterinarians. The carcasses were burned with diesel fuel at special waste disposal sites close to the affected villages or poultry plants, and the sites were subsequently decontaminated with bleach according to procedures specified in the special veterinary biosafety manual.
- More stringent regulations were imposed on commercial poultry farms, requiring the establishment of well-regulated sanitary control measures, preven-

TABLE 10-1 Data on Pathogenicity of Various Avian Influenza Virus Strains in Mice (Onishchenko* et al., 2006; Lipatov et al., 2007)

Virus strain	IgEID ₅₀	IgMID ₃₀	IgMLD ₅₀	Organs (in Ig of titer)					
				Lungs	Spleen	Brain	Liver	Kidneys	
A/Gs/Krasnozerskoye/627/05	9.2	2.2	2.3	6.1	1.6	5.2	1.6	2.6	
A/Tk/Suzdalka/1-12/05	9.3	5.3	6.3	4.1	<1	2.3	<1	<1	
AVN/1204*	9.8	2.3	3.8	6.9	3.4	2.2	<1	<1	
A/Ck/Indonesia/05*	9.3	5.3	>7	4.3	<1	<1	<1	<1	

tion of any contacts between domesticated and wild birds, thermal treatment of feed, and so forth.

- Spring and autumn hunting of wild fowl was prohibited or limited, and all hunters were notified of the need to incinerate the intestines and feathers of any fowl taken.
- The most stringent limitations or prohibitions were placed on transportation of live domesticated birds and their meat from region to region.
- Domesticated birds were vaccinated in all areas where avian influenza epizootics were recorded in 2005. The village of Reshety, where the inhabitants refused to vaccinate their birds, was the only site in western Siberia that suffered from avian influenza. Already in 2007, all inhabitants of Novosibirsk Oblast agreed to vaccinate their birds.

In 2007, avian influenza outbreaks were recorded only in the European part of Russia:

- The Republic of Adygeya in Krasnodar Krai: There were several outbreaks among domesticated birds on individual farms in January-February, with the recovered strains shown to be closely related to strains isolated in Azerbaijan and Turkey in the fall of 2006.
- Nine regions of Moscow Oblast in February (in domestic fowl kept in yards): Several suspicious human cases were recorded; however, other causes of acute respiratory diseases were found. The outbreak in Moscow Oblast was most likely caused by poultry illegally transported from Krasnodar, as was demonstrated by examining the nucleotide sequences of recovered avian influenza virus isolates.
 - Krasnodar Krai in September (in domesticated birds on a private farm)
 - Rostov Oblast in December (in domesticated birds on individual farms)

Note that stringent sanitary measures in combination with the vaccination of domesticated birds and other measures considerably decreased the number and scale of epizootics recorded in European Russia in 2007 and allowed epizootics in Asian Russia in 2007 to be avoided entirely.

It should also be highlighted that the situation regarding this disease in wild and domestic fowl in China in 2007 was rather unusual: No epizootics were recorded in the Qinghai Lake region. Presumably that is why migratory birds flying north in the spring to Russia and Kazakhstan carried no influenza viruses. On the other hand, no epizootics occurred in the Chinese provinces where human cases were recorded, which is quite unusual. There were reports in the media about the mass vaccination of domestic birds in China in the spring of 2007, but authors have no data about the scale of the vaccination effort or the vaccine composition and type.

Thus, humankind has sufficient measures for controlling epizootics caused by the H5N1 avian influenza virus. Mortality of domesticated birds on individual farms can be minimized and on commercial closed-type poultry farms can be completely excluded in countries where all antiepidemic measures are carried out, the public is kept informed about ways of minimizing the risk of domestic fowl infection, and birds are vaccinated.

However, it should be kept in mind that avian influenza is not the only emerging disease and that migratory birds are only one potential source for the appearance and spread of emerging infections. Other possible sources are discussed in the following sections.

HUMAN COLONIZATION OF NEW TERRITORIES INHABITED BY ANIMALS OR INSECTS PREVIOUSLY UNKNOWN TO HUMANS (TICK-BORNE ENCEPHALITIS IN 1937-1940 IN THE RUSSIAN FAR EAST)

When people enter new and previously unexplored territories, pathogens can be transferred from animals or insects to humans. This happened in the late 1930s in the Russian Far East during construction of the Khabarovsk–Komsomolsk-na-Amure railroad. During this project, tens of thousands of people worked in the taiga, where virtually no people had been present before. During the first year of construction, mass human cases of encephalitis were recorded. To clarify the underlying reasons, several expeditions of researchers and experts headed by the outstanding Russian scientists L. A. Zilber, E. V. Shibladye, E. Pavlovsky, A. A. Smorodintsev, and M. P. Chumakov were sent to the area. The expeditions discovered that ticks were the vector for the pathogen in question. Measures for controlling ticks and avoiding tick bites were immediately implemented. Special clothing was designed for workers, and the practice of regular mutual tick examinations every 3-4 hours was introduced. Consequently, the morbidity rate was considerably reduced. Later, a vaccine against this disease was developed. This disease is today controllable by vaccination, and only the insufficient level of vaccination among the population is the reason for tick-borne encephalitis morbidity in Russia (up to 7,000 cases annually). However, it should be noted that tick-borne encephalitis virus continues to spread not only in Russia but also in other countries in northern and central Europe and Asia, including Germany, Austria, Switzerland, the Czech Republic, Kazakhstan, and others. Vaccination against tick-borne encephalitis is therefore becoming increasingly widespread in these countries.

INDUSTRIAL BREEDING OF RARE ANIMAL SPECIES (PALM CIVET AND SARS CORONAVIRUS)

Today it is well known that the commercial breeding of rare palm civets for their meat was the source of severe acute respiratory syndrome caused by SARS coronavirus in China. The Chinese recently started eating palm civet meat and breeding the animals, and civets frequently carry the coronavirus. Researchers have discovered that a random deletion of an insignificant portion of the gene encoding a key protein (less than 0.1 percent of the genome) and several nucleotide substitutions made this coronavirus infectious for humans. When consumption of civet meat and commercial breeding of the animals were halted, human contact with these animals also stopped, as did the epidemics caused by the coronavirus in question.

INTRODUCTION OF NEW ANIMALS TO NEW TERRITORIES

Several animal species—muskrat, American mink, and nutria—were imported to Russia in the 1930s, initially for captive breeding. These species later successfully acclimatized in the wild. Cases of Omsk hemorrhagic fever appeared in the area inhabited by muskrat 20 years after this species appeared there. Sequencing of the genome of Omsk hemorrhagic fever virus demonstrated that it was very closely related to the tick-borne encephalitis virus. During the past 30 years, cases of Omsk hemorrhagic fever were recorded only among muskrat hunters. Presumably, this means that muskrat had become the natural host of this virus.

As for American mink and nutria, we do not yet know the particular pathogens that can be transmitted from these animals to humans; however, it is quite possible that scientists may discover either new or changed pathogens that came to Eurasia from the American continent with mink or nutria or that have changed during passaging in these species.

CLIMATE CHANGE (WEST NILE AND JAPANESE ENCEPHALITIS VIRUSES IN SIBERIA)

Global warming and resulting climate change creates conditions appropriate for reproduction of more southern insect species on territories with previously severe climate, and these insect species that are new to particular areas appear able to transmit diseases that have not been transmitted by the insects that have long inhabited these areas. As just one example, West Nile virus is now detectable not only in the European part of Russia but also in western Siberia and the Russian Far East; moreover, it is found not only in birds and mosquitoes but also in human encephalitis cases. Most likely, this represents a more global process than seemed the case 2 or 3 years ago, as a considerable level of antibodies to this virus was detected in the human population in 2007, amounting to 20 percent of

the population in certain regions of western Siberia. In addition, isolated cases of Japanese encephalitis are being recorded in the Russian Far East (earlier, this disease was very rare in Siberia). All these facts suggest that climate change as a result of global warming not only can cause thawing of permafrost and ice but can also lead to the emergence of tropical diseases in new areas due to propagation of insect species that are vectors of these diseases.

UNINTENTIONAL CREATION OF NEW CONDITIONS FOR PROPAGATION OF ANIMALS AND INSECTS

It is known that dog and wolf populations in trash dumps increase rapidly if not controlled, thereby allowing for reproduction of dangerous diseases such as rabies. Unfortunately, this situation has occurred recently in several cities of western Siberia, and only intensive control of stray dogs has reduced the number of infected animals in the neighborhoods of these cities.

As for other analogous processes, experts noted long ago that mosquitoes reproduce very intensively in used tire dumps because of favorable conditions created inside the tires. This situation can also be threatening for Siberia, as crowds of mosquitoes appearing in tire dumps in combination with the animals inhabiting the same sites can form reservoirs for a multitude of infections, including malaria. Fortunately, malaria is still not endemic in Russia, but if further climate change occurs, it may become endemic, which would have dramatic consequences given the huge territory and many lakes, ponds, and marshes in Siberia and in Russia as a whole.

ADOPTION OF NEW TECHNOLOGIES

Adoption of household technologies new to a particular region can also be a reason for the emergence of new infections. In particular, it was known in Russia that Legionnaire's disease cases were recorded abroad; however, no cases were found in this country until recently. On the other hand, humidifying air conditioners were virtually absent in Russia until the 1990s; therefore, the specific conditions for cultivation and reproduction of the corresponding bacteria were also absent. Today, such air conditioners are present not only in offices but also in apartments, so cases of Legionnaire's disease have consequently appeared. In western Siberia, such cases were recorded in Biisk (Altai Krai) 3 years ago. Several dozen Legionnaire's disease cases were recorded in Yekaterinburg and neighboring cities in 2007. Some were associated with air conditioners and some with stagnant warm tap water that was also polluted, conditions that enhanced reproduction of legionellosis bacteria and subsequent human infection.

CONCLUSIONS

Reproducing intensively and colonizing new territories, humankind itself creates new possibilities for the reproduction, spread, and variation of infectious pathogens. Correspondingly, it is necessary to take into account all the possible reasons that bring about new infections in order to prevent their emergence or minimize their consequences. In particular, monitoring acute zoonotic and potentially zoonoanthropotic infections in wild animals and birds in areas close to their habitats and migratory pathways in Russia and the other countries of the Commonwealth of Independent States (CIS) is most useful for preventing the spread of emerging infections. This is also very important for European countries, as migratory birds during one season transfer the pathogens reproducing in them over vast territories. One of the most important rest stops and nesting grounds for birds migrating to Eurasia is located in the southern part of western Siberia (Chany Lake and other lakes of Altai Krai and Omsk and Novosibirsk oblasts). Therefore, it is most important to monitor and study the pathogens of various infections in migratory birds and wild animals in these particular regions, as they will appear in these regions somewhat earlier than they will become dangerous for people. Further strengthening Russian research potential in this field is vital for providing early alerts of new emerging infections for Russia, other CIS countries, European and Asian countries, and even the United States and Canada, as the so-called Palearctic migratory flyway goes from Siberia to Alaska, so migratory birds can potentially transfer pathogens all over the American continent. Therefore, joint research on infectious agents, especially zoonotics, in Russia and the United States will assist both countries in countering new threats of emerging infections. We are well aware that only one emerging infection—avian influenza—has claimed more than 160 lives during the past 6 years, whereas bioterrorism is to blame for only six deaths during that time. This means that Nature is still the world's chief bioterrorist. An increase in our joint potential in the control of emerging and yet unpreventable infections will contribute to public health in our nations and in neighboring countries and provide us with more options for combating any kind of bioterrorism, be it deliberate or generated by nature.

REFERENCES

- Evseenko, V. A., A. V. Zaikovskaya, V. A. Ternovoi, A. G. Durimanov, S. I. Zolotykh, Y. N. Rassadkin, A. S. Lipatov, R. G. Webster, A. M. Shestopalov, S. V. Netesov, I. G. Drozdov, and G. G. Onishchenko. 2007. Diversity of highly pathogenic avian influenza H5N1 viruses that caused epizootic in western Siberia in 2005. *Doklady Biological Sciences* 414:226-230.
- Ilyinskikh, E. N., I. N. Ilyinskikh, and A. V. Lepekhin. 2008. The first cases of West Nile fever in Tomsk region. Materials of the scientific and practical conference "Actual problems of tick borne infections." *Medicine in Kuzbass* 6:75-76 (in Russian).

- Kononova, Yu. V., A. G. Mirzaeva, Yu. L. Smirnova, E. V. Protopopova, T. A. Dupal, V. A. Ternovoi, Yu. A. Yurchenko, A. M. Shestopalov, and V. B. Loktev. Species composition of mosquitoes (Diptera, Culicidae) and possibility of the West Nile virus natural foci formation in the south of Western Siberia. *Parasitology* 41(6):459-470 (in Russian).
- Lipatov, A. S., V. A. Evseenko, H. L. Yen, A. V. Zaikovskaya, A. G. Durimanov, S. I. Zolotykh, S. V. Netesov, I. G. Drozdov, G. G. Onishchenko, **R. G. Webster, and A. M. Shestopalov. 2007.** Influenza (H5N1) viruses in poultry, Russian Federation, 2005-2006. *Emerging Infectious Diseases* 13(4):539-546.
- L'vov, D. K., M. Yu. Shchelkanov, P. G. Deriabina, T. V. Grebennikova, A. G. Prilipov, E. A. Nepoklonov, G. G. Onishchenko, N. A. Vlasov, T. I. Aliper, A. D. Zaberezhny, D. E. Kireev, O. P. Krashennnikov, S. T. Kiriukhin, E. I. Burtseva, and A. N. Slepushkin. 2006. Isolation of influenza A/H5N1 virus strains from poultry and wild birds in West Siberia during epizooty (July 2005) and their depositing to the state collection of viruses (August 8, 2005). *Advances in Virology* 51(1):11-4 (in Russian).
- Onishchenko, G. G., S. P. Bereznev, A. M. Shestopalov, A. Yu. Alekseev, V. A. Ternovoi, A. B. Khaitovich, M. T. Krovyakova, S. V. Netesov, and I. G. Drozdov. 2007. Molecular biologic analysis of avian influenza virus isolates which caused epizootics on the south of West Siberia and in Crimea. *Zh Microbiology, Epidemiology, and Immunobiology* 5:28-32 (in Russian).
- Onishchenko, G. G., A. M. Shestopalov, V. A. Ternovoi, V. A. Evseenko, A. G. Durimanov, Yu. N. Rassadkin, Yu. V. Razumova, A. V. Zaikovskaya, S. I. Zolotykh, S. V. Netesov, and L. S. Sandakhchiev. 2006. Highly pathogenic influenza virus H5N1 found in western Siberia is genetically related to viruses that circulated in Southeast Asia in 2003-2005. *Doklady Biological Sciences* 406:63-65.
- Onishchenko, G. G., A. M. Shestopalov, V. A. Ternovoi, V. A. Evseenko, A. G. Durimanov, Yu. N. Rassadkin, A. V. Zaikovskaya, S. I. Zolotykh, A. K. Yurlov, V. N. Mikheev, S. V. Netesov, and I. G. Drozdov. 2006. Study of highly pathogenic H5N1 influenza virus isolated from sick and dead birds in Western Siberia. *Zh Microbiology, Epidemiology, and Immunobiology* 5:47-54 (in Russian). Erratum in *Zh Microbiology, Epidemiology, and Immunobiology* 7:128.
- Shestopalov, A. M., A. G. Durimanov, V. A. Evseenko, V. A. Ternovoi, Yu. N. Rassadkin, Yu. V. Razumova, A. V. Zaikovskaya, S. I. Zolotykh, and S. V. Netesov. 2006. H5N1 influenza virus, domestic birds, western Siberia, Russia. *Emerging Infectious Diseases* 12(7):1167-1169.

Activities of the Russian Federal Medical-Biological Agency Related to Radiation, Chemical, and Biological Security*

Vladimir V. Romanov, Deputy Head of the Russian Federal Medical-Biological Agency (FMBA) and Chief State Sanitary Physician for Organizations and Territories Served by FMBA

Organizationally, the Russian Federal Medical-Biological Agency (FMBA) is a unified complex of clinical, prophylactic, sanitary, antiepidemic, and research organizations whose activities are aimed at improving working conditions for personnel in especially hazardous industries and detecting and eliminating the effects of harmful physical, chemical, and biological factors on the health of workers and the public living near dangerous facilities. The agency includes 92 clinical-prophylactic facilities (central medical-sanitary units, medical-sanitary units, and clinical hospitals), 19 scientific research institutes, 42 regional (inter-regional) offices, and 63 hygiene and epidemiology centers.

Celebrating its 60th anniversary in 2007, FMBA is the successor of the Third Main Administration of the USSR Ministry of Health, which was organized in 1947 to provide medical and sanitary-hygiene support for efforts to create nuclear weapons. The administration was later assigned tasks related to monitoring working conditions for chemical weapons industry workers and for handling disease-prevention measures both for manned space flights and for organizations working with pathogenic microorganisms in hazard classes 1-4.

*Translated from the Russian by Kelly Robbins.

In accordance with existing Russian Federation legislation, FMBA is responsible for medical-sanitary support functions and state sanitary-epidemiological monitoring for organizations in certain industries in which working conditions are particularly hazardous and for the population in certain areas (Decree of the Russian Federation President No. 1304, On the Federal Medical-Biological Agency, dated October 11, 2004; Russian Federation Government Resolution No. 789, Issues Regarding the Federal Medical-Biological Agency, dated December 15, 2004; and Russian Federation Government Resolution No. 206, On the Federation Medical-Biological Agency, dated April 11, 2005). It also performs state regulatory functions related to the use of nuclear power (Russian Federation Government Resolution No. 412, On Federal Executive Branch Agencies Involved in State Management of the Use of Nuclear Power and State Regulation of Safety in the Use of Nuclear Power, dated July 3, 2006). There is no comparable organization in the United States that focuses on very hazardous environments at nuclear, chemical, and biological facilities.

According to Russian Federation government directives (No. 1156-r of August 21, 2006, and No. 1745-r of December 16, 2006), the list of entities served by FMBA includes all of the main radiation-, chemical-, and biological-hazard organizations operating under the auspices of the Federal Atomic Energy Agency, the Federal Industrial Agency, the Federal Oversight Service for the Protection of Consumer Rights and Human Welfare, and other executive branch agencies of the federal government and the various jurisdictions in which those organizations are located.

FMBA carries out its activities both directly and through its subsidiary local monitoring offices and organizations. The local offices and FMBA hygiene and epidemiology centers are part of the unified system of agencies and institutions responsible for state sanitary-epidemiological oversight in the Russian Federation. Policies and procedures governing their activities are set forth in Russian Federation Government Resolution No. 569, Statute on the Provision of State Sanitary-Epidemiological Oversight in the Russian Federation, dated September 15, 2005.

The scientific research institutes under FMBA's auspices provide scientific support for the activities of the agency's practical health care institutions, local offices, and hygiene and epidemiology centers. They study the health status of assigned populations and provide state sanitary-epidemiological oversight in the development of regulatory-legal acts on monitoring of organizations presenting radiation, chemical, and other hazards.

Furthermore, FMBA's scientific research institutes have produced fundamental results in studying the effects of ionizing radiation on the human body, radiobiology, and radiation medicine and hygiene and in developing medical preparations that protect against radiation and chemical impacts and individual gear and devices that protect the respiratory systems and skin of workers at radiation-hazard facilities. The institutes have also made progress in the area of

biological instrument manufacturing, new-generation vaccine development, and research on the immune status of workers at hazardous facilities, among other developments.

The State Science Center—Institute of Biophysics includes Russia's only clinical department specializing in the treatment of radiation-related conditions (the Occupational Pathology Department) and also features an emergency medical dosimetry center. The center was created as an emergency response unit. It is functionally included in the Federal Atomic Energy Agency's Crisis Center and is responsible for providing support for the activities of FMBA local offices and institutions in the assessment of the radiation situation in areas affected by radiation accidents and in management decision making on emergency response measures by FMBA subunits.

FMBA's accumulated expertise and the many research developments it has made in the areas of radiation, chemical, and biological safety must undoubtedly be used to protect the population of the Russian Federation from the current level of terrorist threats. FMBA is open to cooperation and is prepared to work within the framework of joint U.S.-Russian research projects to prevent threats of high-technology terrorism.

The Problem of Oil and Natural Gas Pipeline Security*

S. G. Serebryakov,

Russian Academy of Sciences Institute of Oil and Gas Problems

The natural gas produced in Russia is transported through major gas pipelines linked to Russia's Unified Natural Gas Supply System (see Figure 15-1), the largest such system in the world. The total length of all pipelines in the system, which belongs to the Open Joint-Stock Company Gazprom, is 156,300 kilometers. It includes 268 compressor stations with a total of 4,078 pumping units with a 44.8 million kilowatt capacity, as well as 3,818 natural gas distribution stations.

As of December 31, 2005, the average length of service for major natural gas pipelines was 22 years. Their stable operation is ensured thanks to the introduction of progressive methods for diagnostics, scheduled maintenance, and repairs. Gazprom is implementing a comprehensive program for reconstruction and technical upgrading of natural gas transmission lines, compressor stations, and underground storage facilities for the period 2007-2010. The primary goals of the program are to improve the efficiency of the gas transmission system, ensure the transport of planned volumes of gas and the reliable operation of the transmission system, and improve the industrial and environmental safety of all its components.

The Unified System is today operating at full capacity. In 2005, Gazprom

*Translated from the Russian by Kelly Robbins.

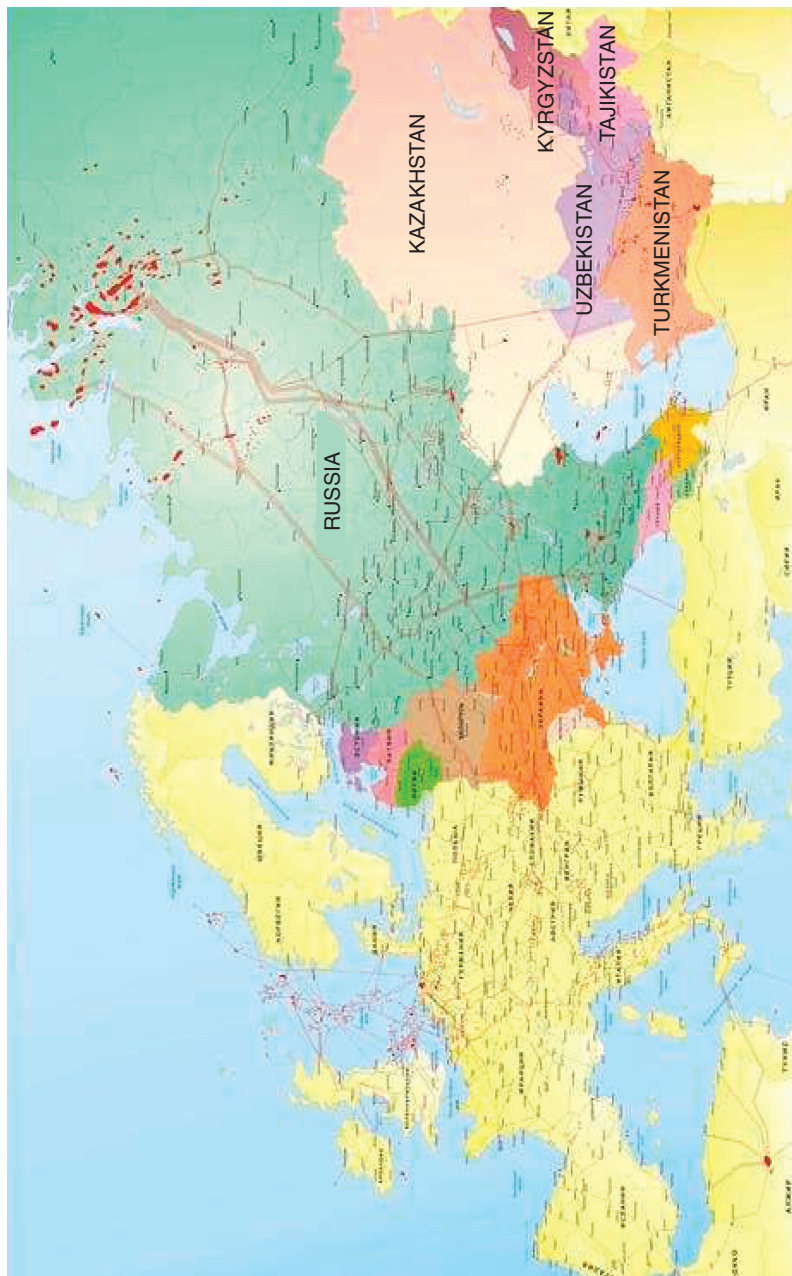


FIGURE 15-1 Russia's Unified Natural Gas Supply System.

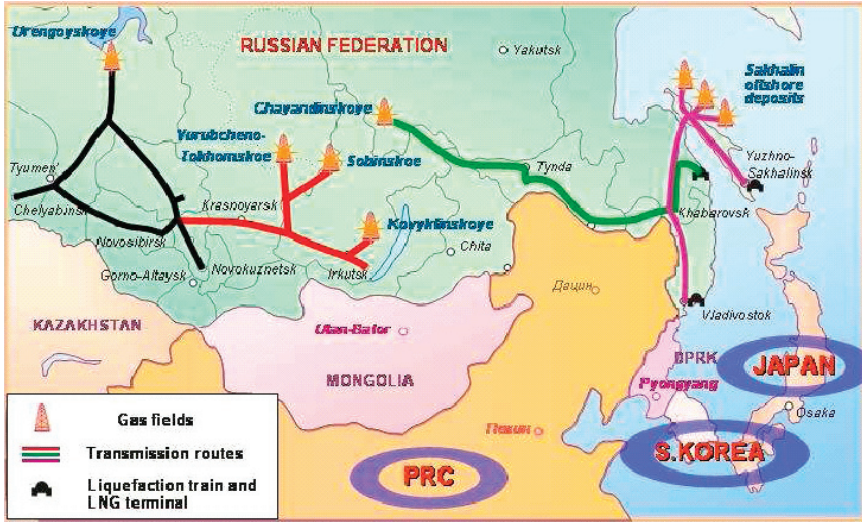


FIGURE 15-2 Planned routes of major natural gas pipelines.

extracted 547.9 billion cubic meters of natural gas. Taking into account independent producers and those from the Central Asian states, the system transported a total of 699.7 billion cubic meters of natural gas. Even today its transmission capacity needs to be increased by 35 billion cubic meters, with further increases necessary in the future, given that by 2020 Gazprom plans to extract 580-590 billion cubic meters of natural gas with up to an additional 170 billion cubic meters from independent producers. The planned routes of the major gas pipelines are shown in Figure 15-2.

The 24 underground natural gas storage facilities located in areas of major gas demand are an essential element of the Unified System. They make it possible to handle seasonal fluctuations in natural gas demand, reduce peak system loads, and ensure flexible and reliable gas transmission. Three underground storage facilities are under construction, including one near Volgograd that will be the largest of its kind in Europe, with a volume of 800 million cubic meters and a daily output capacity of 70 million cubic meters.

With a total length of more than 46,000 kilometers, the Transneft company's unified system of major oil pipelines (see Figure 15-3) transports 99.5 percent of all oil produced in Russia both to refineries and for export to the countries of the Commonwealth of Independent States, Poland, Germany, Slovakia, and Hungary through the Druzhba oil pipeline system and through deep-water oil transfer terminals on the Black and Baltic seas. Transneft serves a territory twice as large as



FIGURE 15-3 Unified system of major oil pipelines of Transneft and nearby foreign countries.

that of the U.S. oil supply system and provides transport services to oil-producing enterprises in the republics of Kazakhstan and Azerbaijan.

At the end of 2005, the total length of Russia's major pipelines was more than 231,000 kilometers, including the following:

- Major natural gas pipelines: 161,100 kilometers
- Major oil pipelines: 49,000 kilometers
- Major refined product pipelines: 19,500 kilometers
- Ammonia pipelines: 1,400 kilometers

All of these facilities present a significant danger to personnel, the public, and the environment.

A report submitted in 2005 by the Russian Federal Service for Environmental, Technological, and Nuclear Oversight (FSETNO) shows that the following factors present the primary threats to the integrity of major pipeline transmission facilities:

- Intensive development of stress corrosion processes on large-diameter major natural gas pipelines due to deterioration of the protective sealant coating the pipelines, which were constructed 15 or more years ago. Whereas from 1991 through 1996, the rate of accidents due to this cause was about one-fourth of all accidents in the Gazprom system; from 1998 through 2003, accidents due to this cause represented one-third of the total; and in 2005 this figure was already more than 50 percent.

- Significant growth in the number of cases of unauthorized connections to oil and petroleum product pipelines with the aim of stealing the products being transported. This increase in thefts has been particularly acute in the republics of Dagestan and Chechnya; Samara, Nizhny Novgorod, and Saratov oblasts; and Stavropol and Krasnodar territories.

- Accidents due to shoddy construction and installation work resulting from the lack of an effective system of technical monitoring of design specification compliance during intensive construction of major pipeline transport facilities in the 1970s and 1980s.

An analysis conducted by FSETNO of the results of investigations of accidents occurring in 2005 is presented in Table 15-1.

Table 15-2 presents FSETNO's analysis of accident and injury statistics for major pipeline transport operations for 2005 compared with the same figures for 2004.

The most significant accidents in 2005 were those at the Petrovsk-Yelets main natural gas pipeline on January 18, 2005, and the Khadyzhensk-Psekupskaya-Krasnodar main oil pipeline on August 7, 2005.

On January 18, 2005, the major natural gas pipeline Petrovsk-Yelets (built

TABLE 15-1 Results of Investigations of Accidents in 2005

Cause	Natural Gas Pipelines	Oil Pipelines	Product Pipelines	Total
1. External mechanical impacts, including	3	12	5	20
Cutting	–	8	1	9
Construction equipment	3	4	4	11
Terrorism	–	–	–	–
2. Corrosion damage	14	–	–	14
3. Shoddy construction or installation work	3	2	–	5
4. Operator error	1	–	1	2
5. Defective parts or materials received from manufacturer	2	2	–	4
Total	19	13	3	45

TABLE 15-2 Accident and Fatal Injury Rates for Major Pipeline Operations in 2004 and 2005

Pipelines	Number of accidents			Number of fatalities due to injury		
	2004	2005	+/-	2004	2005	+/-
Natural gas pipelines	29	19	–10	2	2	0
Oil pipelines	19	13	–6	3	2	–1
Refined product pipelines	0	3	+3	1	–	–1
Total	48	45	–13	6	4	–2
Total length of pipelines (in thousands of km)	231	231	0			

in 1981 and owned by Gazprom and the Mostransgaz Limited Liability Society) suffered damage at its 316-kilometer mark that blew out 55 meters of pipe and caused the gas to ignite. The accident resulted from the formation during pipeline operations of lengthwise cracks in the surface of the pipe, which, at the moment of the accident, failed to provide the expected stability and led to the pipeline segment being destroyed. The economic impact of the accident was 3,710,900 rubles.¹

On August 7, 2005, the Khadyzhensk-Psekupskaya-Krasnodar main oil pipeline began discharging oil into the Chiby Canal at its 80-kilometer mark in the Republic of Adygeya. The accident was caused by thieves making unauthorized

access to the pipeline to steal oil. The costs of dealing with the accident and its consequences totaled 3,732,185.54 rubles.²

To ensure the industrial safety of the major pipeline transport facilities of Gazprom, Transneft, and Transnefteprodukt, the Comprehensive Programs for Facility Diagnostics, Technical Upgrades, Reconstruction, and Major Repairs have been developed and coordinated with FSETNO and are currently being implemented.

It must be noted that protecting pipelines from terrorism has taken on increasing significance in recent years, particularly after September 11, 2001.

The results of FSETNO inspections in 2005 of the level to which hazardous production facilities are protected against terrorist acts showed that on the whole, all enterprises with such facilities have developed a system of measures to prevent terrorist acts and have made agreements with specialized services to protect them. The grounds of the most important facilities are surrounded by fences or other protective barriers. Meanwhile, many facilities (wells, pipelines, and so forth) are unprotected; therefore, measures are in place for them to be patrolled regularly. All facilities are equipped with telephone hotlines directly connected to emergency services and security dispatch centers. Plans for new hazardous facilities include the installation of external video observation centers.

Individual terrorist acts have been carried out against pipelines in Russia, primarily during the period of military actions in Chechnya. On April 15, 1996, a bombing severed a major natural gas pipeline 1,200 millimeters in diameter on the left bank of the Terek River in Shelkovskaya Region in the Republic of Chechnya. When the explosive device was detonated near where the gas pipeline emerges from underground, the entire pipeline was blown off its supports. The blast produced a crater 33 by 29 meters in area and 10 meters deep. The pipeline break led to a fire that burned a total of 25,000 square meters on both banks of the Terek River.

On June 14, 1999, sabotage caused an accident at the 124-kilometer mark on the linear portion of the Grozny-Baku main oil pipeline, which is owned by the Open Joint-Stock Company Chernomortransneft and the Stock Company Transneft. Placed in service in 1983, the Grozny-Baku oil pipeline has an operating pressure of 4.3 megapascals and transports a mixture of Azerbaijani and Dagestani oil. The raised segment of the pipeline at its 124-kilometer mark in the Yaryk-Su River bed is suspended on supports and constructed of pipe that is 720 millimeters in diameter. The accident was caused by the energy effects of an explosive device placed under the pipeline. A total of 199 cubic meters of oil (169 metric tons) was spilled, contaminating about 3 hectares of nearby territory in the river basin. The costs of dealing with the accident and its consequences totaled 664,896 rubles.³ These examples provide a graphic demonstration of the damages caused by terrorist attacks.

The potential terrorist threat and the increased number of cuts in oil pipelines for the purpose of unauthorized removal of oil have required Transneft to take

certain measures to prevent damages to elements of the energy infrastructure. In 2000 the company began working to create a concept for an effective vertically integrated corporate security system. It created the Security Systems Department, including mobile armed groups and economic security subunits for the company as a whole and for its subsidiaries, to provide physical protection for oil transport facilities. To prevent pipeline damage and oil thefts due to unauthorized pipeline cuts, the Security Systems Department is introducing several technical capabilities and closely tracking all modern research developments in this field both in Russia and abroad. In recent years, security equipment has been installed at 78 percent of the company's facilities.

Pipelines present a convenient target for terrorists, inasmuch as a simple explosive device can knock them out of commission for weeks. It is for this reason that they have become the focus of sabotage in Iraq.

According to information from the Institute for the Analysis of Global Security (United States), since the end of the war declared by George Bush in April 2003, 37 attacks on pipelines, oil facilities, and their personnel were recorded in 2003, 147 in 2004, 100 in 2005, 100 in 2006, and 5 in January 2007. Most of these attacks occurred on pipelines leading to Turkish and Syrian terminals on the Mediterranean Sea, at the Bayji refinery complex 200 kilometers north of Baghdad, and at oil facilities south of Basra, where more than two-thirds of Iraq's oil is extracted (see Figure 15-4).

Iraq's proven oil reserves total 15.5 billion metric tons (9.6 percent of world reserves), ranking the country fourth behind Saudi Arabia, Russia, and Iran. Meanwhile, after falling to 65.7 million metric tons in 2003 and rising to 99.2 million metric tons in 2004, oil production again fell by 10 percent to 89.5 million metric tons in 2005. Iraqi oil could take the pressure off world markets in the face of high demand by China, the problems with Iran's nuclear program, and unrest in Nigeria's oil-producing region in the Niger Delta. However, the country is not even meeting its own domestic needs. As a result, Iraq imports refined petroleum products at very high prices at the same time that it could be increasing its own oil exports and earning money to restore its economy.

"Every day that oil shipments are paralyzed costs us \$60 million," Iraqi oil minister Tamir Gadban has declared. All of this has caused Iraq to lose more than \$10 billion from oil sales, undermined prospects for the country's reconstruction, and led to a situation in which oil companies are not taking the risk of investing in the development of the Iraqi oil and gas industry.

The success of terrorist acts in Iraq has led terrorists in other oil-producing countries to turn their attention to pipelines and other oil industry facilities. In December 2004, insurgents attacked an oil field in Sudan. In India, separatists claimed responsibility for several attacks on oil pipelines in the state of Assam, the source of about 15 percent of India's oil output. Rising demand for oil in the country makes its economy increasingly sensitive to supply disruptions. In Turkey, Kurdish partisans carried out a series of strikes against oil pipelines. At-

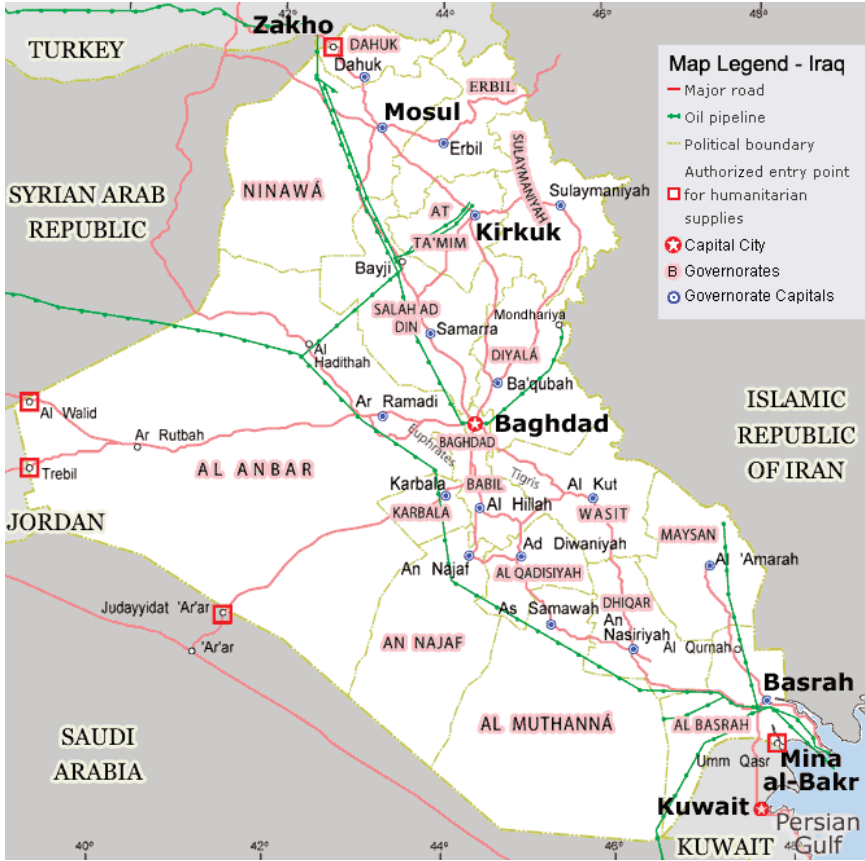


FIGURE 15-4 Map of Iraq’s oil pipelines.

tacks on oil-drilling platforms in Nigeria in 2006 led to a halt in oil production in that country.

However, the greatest disruptions in oil supplies to the world market would be caused by actions against the oil pipelines of Saudi Arabia, which produces about 25 percent of the world’s oil and which has about 17,000 kilometers of pipelines throughout the country, primarily located underground.

Economists have calculated that the risk of terrorist attacks has already caused the price of oil to rise by about \$10 per barrel as a sort of insurance premium. Terrorists clearly understand that oil price increases as a result of sabotage against oil and natural gas pipelines are felt very keenly not only by the U.S. economy, which lost about \$40 billion for this reason in 2004, but also by the world economy.

The most obvious way to provide increased security for pipelines is to establish security patrols and create buffer zones along their routes in which unauthorized access is prohibited. In Iraq an entire army of 14,000 guards has been deployed along pipelines and at oil wells and refineries.

Systems for detecting irregularities and complex modern systems for monitoring particularly vulnerable points could play an important role in protecting pipelines. These systems, which use supersensitive seismic monitoring devices, could provide early warnings if saboteurs were to approach a protected area. Such remote monitoring systems for the pipeline network could be very expensive; however, they would make it possible to avoid the costs of supporting a significant contingent of troops to protect the network, as personnel needs would be limited to small rapid-response groups.

These systems could be augmented by observation from the air, including using pilotless drones capable of flying for up to 30 hours at medium and low altitudes and transmitting high-resolution images to a central station for subsequent processing. There have been reports of the development of pilotless aircraft equipped with automatic weapons, which could be used against saboteurs. Unfortunately, the majority of countries where such systems would be most effective lack the necessary financial resources to acquire them. In such cases, even fences and walls could be used as protective measures to prevent access to facilities. New pipelines must be laid underground. This increases their construction costs, but the return on investment is rapid. It is also important to reduce the time between pipeline damage and repair; the shorter the time, the less damage is done. With this in mind, it would make sense to reduce the length of damaged pipeline segments that must be repaired.

However, it must be understood that ensuring the security of natural gas and oil pipelines is a rather complex problem, the resolution of which is determined by improved equipment and technology for new pipeline construction, more reliable diagnostics, modern means of rapidly eliminating the consequences of accidents, and, on the other hand, development of effective measures and equipment for preventing terrorist attacks against elements of the oil and gas infrastructure. No matter what new equipment or capability may be proposed, it will only increase the cost of a barrel of oil, which has already reached a colossal level. As long as oil and natural gas are the foundation on which the world economy functions, the threat of such attacks will obviously remain, and new achievements in the sphere of their prevention will inevitably increase the price of a barrel of oil.

NOTES

1. Approximately \$132,343 at the exchange rate prevailing at that time.
2. Approximately \$131,323 at the exchange rate prevailing at that time.
3. Approximately \$26,810 at the exchange rate prevailing at that time.