Counter-Terrorism Capability: Preventing Radiological Threats

Vladimir Lukov *

Introduction of a New Phenomenon of Global Mini-Terror

For many decades, terrorism was perceived as a contest between two sides: on the one hand, a group of people or an organization, and on the other, a sovereign state. However, during the course of the second half of the twentieth century, various countries began to use terrorist organizations to promote state interests in the international domain. In some cases, states have established "puppet" terrorist organizations, whose purpose is to act on behalf of the sponsoring state, to further the interests of the state, and to represent its positions on either the domestic or regional front. In other cases, states sponsor existing organizations on the basis of mutual interests.

The patron state provides its beneficiary terrorist organization with political support, financial assistance, and the sponsorship necessary to maintain and expand its struggle. The patron uses the beneficiary to perpetrate acts of terrorism as a means of spreading the former's ideology throughout the world, or in some cases, the patron ultimately expects the beneficiary to gain control of the state in which it resides or impart its ideology to broad sections of the general public.

State-sponsored terrorism can achieve strategic ends in cases where the use of nuclear and conventional armed forces is not practical or effective. The high costs of modern warfare, and concern about non-conventional escalation, as well as the danger of defeat and the unwillingness to appear as the aggressor, have turned terrorism into an efficient, convenient, and generally discreet weapon for attaining state interests in the international realm.

Now the main role in playing the card of radiological terrorism seems to belong to small mini-terror devices**.** For example, representatives or supporters of failed regimes, rogue states, and other non-state actors may take hand-grenades and connect them to bags filled with radiological materials. That is the simplest description of a so-called "dirty bomb."

Today the greatest threat for Russia, the U.S., and NATO is the possibility of a secret and sudden attack with radiological or improvised nuclear weapons. Many analysts have come to the common conclusion that from now on there is a new phenomenon in the arenas of global policy and economy, namely global terrorism.

The actors of global terrorism possess a non-state status. It consists of failed and disaffected states, ethno-religious terrorists, greedy and socially irresponsible proliferators, narco-traffickers, and other organized criminals, who are taking advantage of the new high-speed information environment and other advances in technology to integrate their illegal activities and compound their threat to stability and security around the world. Radiological terrorism is one of the most potentially effective

* Dr. Vladimir Lukov is Senior Science Editor, Minatom.

among a wide array of cheap and unpredictable tools of global destabilization. While a radiological dispersal device (RDD), or a "dirty bomb," could be used as an element of terror, its potential effects cannot be compared with the catastrophic consequences of a nuclear, chemical, or biological weapon. But the public does not necessarily perceive the difference.

Over the coming years, the post-September-11 syndrome is going to create much confusion in the objective understanding of the security threats posed by radioactive sources. That is the core of the problem, which can be solved not by building old-style anti-terrorism capacities, but by taking preventive action—in short, in building a counter-terrorism capability.

Passive Anti-Terrorism and Active Counter-Terrorism

Nuclear security has given rise to countermeasures, such as nuclear material control and physical protection. For other radioactive materials, including sources, the traditional approach has been to consider security as an integral part of the safety effort, i.e. for the radiation protection of workers and for public safety. The events of 11 September 2001 triggered a reconsideration of the risks for, and consequences of, terrorist acts involving nuclear or other radioactive materials.

So both the existing and the coming dangers of radiological dispersal devices have been recognized. In addition to records of past events in which there was a threat or risk of the dispersal of radioactive material, the International Atomic Energy Agency's (IAEA) Illicit Trafficking Database contains some 470 confirmed cases of illicit nuclear trafficking. There are reasons to believe that the reports to the IAEA cover only a small part of all smuggling cases. It is noteworthy that a majority of the cases appear to involve a criminal element. The purpose, however, is often unknown—whether the goal of the trafficking was financial, environmental, or malevolent use. All in all, the possibility that terrorists would use radioactive materials for malevolent purposes cannot be ignored. Moreover, it is time to treat thieves, smugglers, saboteurs, and terrorists equally. All of them are participants in asymmetric warfare. So they are combatants, not criminals, if they try to deal with fissile materials in any way that leads to terrorist attacks.

Radioactive sources are employed for beneficial purposes throughout the world, in industry, medicine, agriculture, and research. Accidents involving radioactive sources and reports of illicit trafficking in radioactive materials have raised awareness of the safety and security risks posed by sources that are outside effective control. The terrorist attacks of 11 March 2004 in Madrid also triggered a lot of international concern about the potential use of radioactive sources by terrorist groups in Europe.

The terrorist attacks of September 2001 and March 2004 have alerted the world to the potential of nuclear/radiological terrorism. Today the world finds itself on the brink of an outbreak of asymmetrical warfare, characterized by the usage of many mini-components of weapons of mass destruction. Thus, huge military contingents may become useless in such warfare.

For example, numerous caves at Tora Bora in the mountains of Afghanistan have revealed how close terror networks may have come to producing crude radiological

dispersal devices. Although the destructiveness of these "dirty bombs" in terms of loss of life and injuries is much smaller than in the case of a nuclear explosion, the consequences would still be horrible. It would also create enormous panic and chaos among the population, and would have severe psychological effects in big cities where the population is informed about radiation. Less well informed people living in the countryside or in the mountains may live with radiation around till the day they die, unaware that it has been carried there by the wind.

In industrialized countries the costs of a wide-scale evacuation of the affected population, the subsequent cleanup of contaminated property, and the long-term health hazards would be very considerable. It is, of course, impossible to accurately assess the likelihood of an attack with "dirty bombs." But it is precisely for this reason that effective cradle-to-grave control of powerful radioactive sources is urgently needed to protect them against use in terrorist acts, theft, or mishandling. The high number of accidental contaminations with radioactive material in the past two decades points in the same direction. Such measures of protection are passive, and ineffective in deterring terrorists.

The security of radioactive materials has traditionally been relatively light. Hence, there is a clear need to strengthen existing security measures as well as to identify and implement additional measures against the potential malevolent use or accidental misuse of radioactive sources.

Methods of anti-terrorism have changed since the era of sporadic attacks directed against Westerners, for example, from the 1960s to the 1980s. In 2001, a new system of anti-terrorism in nuclear industries appeared to protect nuclear power plants from attacks involving a radiological dispersal device or improvised nuclear device (IND). In response to these concerns, U.S. federal agencies initiated steps to develop a better understanding of the magnitude of the threat and to improve their counter-terrorism capability.

New methods based purely at the technological level are dedicated to the prevention of radiological terrorism. They include: 1) personal radiation detectors, with alarms; 2) hand-held instruments for the detection and identification of radionuclides; 3) radiation detection portal monitors; and 4) portable radiation detection instrumentation.

In fact, all these changes were designed by the IAEA in the 1990s, when they were established as part of the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources. Moreover, there were directives issued by this UN "nuclear watchdog" agency to support the implementation of these standards and launch a model project for upgrading the radiation protection infrastructure in its member states.

These initial declarations were met with a wave of seeming cooperation. At first, more than fifty member states participated in the early phase of this model project, and in recent years the number has increased to more than eighty. In 1998, the IAEA, jointly with the European Commission, the International Criminal Police Organization, and the World Customs Organization, organized a number of international conferences on the safety of radiation sources and the security of radioactive materials.

The Bush Administration in the U.S. found the courage to declare a long-term strategy of pre-emptive strikes at any kind of terrorism, taking special aim at those terrorists who were preparing to use radiological methods. But only a few chosen countries were allowed to participate in the newly formed Proliferation Security Initiative (PSI) group. Why?

As President George W. Bush once said, "America, and the entire civilized world, will face this threat for decades to come. We must confront the danger with open eyes, and unbending purpose. I have made clear to all the policy of this nation: America will not permit terrorists and dangerous regimes to threaten us with the world's most deadly weapons." It is a good idea. But terrorists are making up their own minds, and are looking for "dirty bomb" components everywhere. So the ranks of the PSI are to be enlarged in the same way as NATO has done, but far more quickly and with more material Russian participation.

Russia could start moving in the same direction, with clients of the former Minatom as well as with Russia's new partners in nuclear businesses. Why not? The point is that the U.S. and other NATO countries seem to have become more preoccupied with domestic terrorism than international terrorism since the events of September 11 and March 11.

Of course, the IAEA, and especially leading nuclear nations, constantly make assessments of the threat potential (quantitatively as well as with respect to the characteristic assumptions about the probable targets of radiological incidents) by drawing on the expertise and training of the institutions involved (the human "detectors") and by formulating specific scenarios to be considered (e.g., scrap metal monitoring versus airport passenger scanning, nuclear facility perimeter monitoring versus fast scanning at borders). While security arrangements have been maintained to a pretty good degree all over the world, the effect of this reactive anti-terrorist practice will diminish over time.

It has been estimated that in the United States alone, 500,000 of the two million sources of radioactive material may no longer be needed, and thus could be susceptible to being orphaned or become a target of theft by terrorists. In the European Union, some 30,000 sources are in a similar position.[1] Under these circumstances, properly trained and paid Russian contingents could help NATO in monitoring, identifying, and preventing potential radiological accidents and terrorist attacks abroad. This project needs further consideration and financial support.

Many IAEA member states and several international organizations responded positively to the proposal, and therefore the IAEA decided to conduct regular international conferences on the security of radioactive sources, in addition to its other activities in the field. The findings of conferences held in 2003–4 have been brought to the atten-

[1] R.A. Meserve, "Effective Regulatory Control of Radioactive Sources," National Regulatory Authorities with Competence in the Safety of Radiation Sources and the Security of Radioactive Materials, C&S Papers Series No. 9 (Vienna: IAEA, 2001); M.J. Angus, et al., *Management and Disposal of Disused Sealed Radioactive Sources in the European Union*, Rep. EUR 1886 (Brussels: CEC, 2000).

tion of the IAEA Board of Governors, with the evident (but unspoken) conclusion that previous models of fissile materials protection by police and border guards will be quite useless in the ongoing global war on terror.

It is important to emphasize prevention, instead of the focus of previous efforts to localize the effects of radiological emergencies, if any. Advanced technology helps to reduce faulty operations at nuclear units or in radiological devices. Besides, there are probably up to 30,000 radioactive sources that are out of administrative control worldwide. It is therefore important for responsible authorities to establish systems of Internet monitoring and counter-terrorist preventive systems to block such emergencies before they take place, not to handle them the day after.

New Times and Tools for Counter-Terrorism

In early April 2004, U.S. National Security Adviser Condoleezza Rice practically admitted that for more than twenty years the U.S. had essentially failed in the prevention of domestic and international terrorism. She pointed out the lack of an effective counter-terrorism doctrine in the U.S. According to her, anti-terrorism declarations were all well and good, but they were not properly supported with the development of an effective capability during previous U.S. administrations. Such a conclusion seems to be applicable to many states, expect a few, like Israel, Great Britain, Russia (only in Chechnya), etc.

In order to go about separating anti-terrorism and counter-terrorism, two remarks should be made from a methodological point of view. The first one concerns the problem of definition. Today, many authors and specialists in Russia and NATO, especially Americans, use a variety of terms: "mega-terrorism," "super-terrorism," "terrorism of weapons of mass destruction" (WMD), and—one of the latest—"catastrophic terrorism" (global climate change because of green-house gases from fossil fuel burning). In Europe and Russia, the more classical term—"non-conventional terrorism"—is preferred, referring thus to the use, or the threat to use, nuclear and radiological agents or weapons. The second remark is more substantial. It concerns the effect of non-conventional terrorist attacks and models of their prevention.

Most researchers consider radiological terrorism as a new kind of weapon of mass destruction. Devils may be known and unknown. Between limited or mass destruction non-conventional terrorist attacks and extreme or mass annihilation attacks, there is only one difference. It lies in the number of potential victims of any such attack. Only extreme non-conventional terrorist attacks could produce the destruction of a whole city with many thousands of victims and contaminate a large area for a long period of time. More limited attacks might cause hundreds of deaths, perhaps even more, but only on a limited scale (for instance in a stadium, an embassy, a mall, etc.), and without contaminating the area for a long time.

In any case, the prevention of radiological threats is cheaper than the reduction of the potential damage caused. In the U.S., there still exists an old alarmist tradition to calculate "possible losses" that usually serve to justify high budget expenses for contractors who deal with the recovery of damages in anti-terrorism actions.

In fact, experts on terrorism may not be able to calculate or evaluate the real threat presented in this nuclear/radiological field by terrorist organizations in the short and medium term without the support of analytical smart software. Nevertheless, there are also some figures that are extracted from "hand-made" research from 1998–99.

Since the 1980s, the security and safety of military nuclear sites, civil radiological hospitals, and nuclear power plants increased tremendously. That is why incidents of nuclear terrorism (involving attacks or threats against nuclear facilities and radiological terrorism) sharply declined over the past three decades, from 120 incidents during the 1970s to only 15 in the 1990s. In contrast, the incidence of chemical and biological terrorism showed a gradual but steady rise. In the 2000s, we are witnessing a rise of radiological terrorism all over the world because of its low ratio of cost to effectiveness.

Since the year 2000, threats have represented 55 percent of the incidents; 20 percent were threats to use WMD in terrorist attacks. Of this category, threats to use chemical agents represented the majority of incidents (55 percent), threats to use biological weapons represented 25 percent, and nuclear terrorism threats 20 percent. Threats against particular facilities represented 34 percent of the incidents, all of them threats against nuclear reactors and installations.

According to these calculations, 25 percent of the incidents related to an actual terrorist attack. 13 percent of the incidents referred to actions against facilities of weapons of mass destruction, the majority of them against nuclear facilities, but always when nuclear material was absent from the facility, and thus did not present a real physical danger to the environment. 12 percent of the incidents refer to actual use of non-conventional agents. In this category were included incidents that resulted in casualties, but also incidents in which the perpetrators succeeded in placing the materials at their destination without causing any injuries. 88 percent of the incidents of actual use of agents of mass destruction were incidents of chemical terrorism (these figures seem to be overestimated grossly, and are not the focus of this article).

As to the location of radiological terrorism actions, almost 53 percent of the incidents occurred in the United States, and nearly 28 percent occurred in Europe. The incidents that took place in the Middle East represented only 4 percent of the total. Of those, ten out of twelve were incidents of chemical terrorism, and two were of a biological nature. However, it should be noted that Middle Eastern countries (Egypt, Iraq, Iran, and possibly Sudan) have made relatively massive use of chemical weapons on the battlefield, which means that these countries and their proxies had fewer moral constraints against the use of such weapons. In the 2000s, signs of the transportation of fissile materials unauthorized by the IAEA were tracked down in Niger, Turkey, and many other countries. Some of them became reasons for toppling Saddam Hussein's regime in Iraq in 2003. 10 percent of the incidents occurred in Asia, most in Japan (mainly incidents of chemical terrorism), and less than 2 percent were in South America and Africa.

From the existing data, it is clear that the developed, industrial world—the G-8 countries—has become the main ground for radiological terrorism. The United States is leading the targeted countries. This could mean that the counter-terrorism capability is needed most of all in those countries that are advanced in the development and ex-

ploitation of nuclear energy. The fact that very few incidents were registered in the Middle East and South America could imply that radiological terrorism was less used in areas where conventional terrorism was already widespread and successful.

As to Russia and other CIS countries, the only serious radiological incident—which was a mock or hoax attack—was the placement in a Moscow park on 23 November 1995 of "a radioactive container"—in fact a barrel containing radioactive elements—by Chechen terrorists. The quantity of material in the container and its radioactivity (Cesium-137 used in X-ray equipment and some industrial processes) did not present a serious threat of contamination of the area nor of damage to public health.

At the same time, the danger exists that limited, low-level radiological attacks will be carried out in the near future. The most serious danger is the threat of attacks against existing nuclear/radiological civil facilities in the developed countries, as well as in Russia.

Of course, some passive protective measures are being planned by the IAEA. Ensuring the security of radioactive material is about preventing the loss of control of the material. But no pre-emptive measures are on the horizon of the global nuclear industry. For a very good example, here is a list of proposals made in 2002 by a Nuclear Security Plan of Action:

1. Physical protection of nuclear material and nuclear facilities.
2. Detection of malicious activities involving nuclear and other radioactive materials.
3. State systems for nuclear material accountancy and control.
4. Security of radioactive material other than nuclear material.
5. Assessment of safety/security related vulnerability of nuclear facilities.
6. Response to malicious acts, or threats thereof.
7. Adherence to and implementation of international agreements, guidelines, and recommendations.
8. Nuclear security co-ordination and information management.

But there are doubts that these limitations and protective measures will be sufficient to stop those who pursue radiological terrorism. In short, all previous models of protection of radioactive material allow the member states of the IAEA only to control occupational, medical, and public exposures, as well as to coordinate the necessary actions related to the preparedness for and response to radiological emergencies.[2] In the current security environment, this is not enough.

"Trust and Check-up" Methods in Countering the Radiological Threat

The nature of terrorism has been changing steadily since the end of the Cold War.

[2] A.M. Cetto, "Radioactive Sources: The IAEA Model Project as a Case Study," report in the proceedings of an international conference held in Vienna, Austria, 10–13 March 2003, organized by the International Atomic Energy Agency, 219–40. See also an analytical report by Brian Dodd and Eric Reber, "Initiatives by the International Atomic Energy Agency to Prevent Radiological Terrorism," International Atomic Energy Agency.

Many factors are driving this change, including the erosion of national borders, the increasing ease of travel, the revolution in information technology, and the proliferation of weapons of mass destruction. Preventing terrorist activity very much depends on the collection, analysis, and dissemination of information and intelligence, and on cooperation between different jurisdictions, levels of government, and the private sector.

As Henry Kissinger put it recently (12 April 2004), terrorists want to disrupt global market relations where they have no standing or hopes to gain profitable positions in the future. This economic aspect of global terrorism has been consistently camouflaged with anti-Arab, anti-Muslim, etc. hysterics, which often serve the commercial and financial interests of players in the global markets.

In response, terrorists have started to pay more attention to "domestic" stores of radiological materials for future strikes at democracy and free markets in the post-industrialized world, which is rapidly developing nuclear energy as an alternative to fossil fuels. All these changes in the nature of terrorism and the methods of its worldwide activity demand a new, internationally accepted doctrine of counter-terrorism, backed up by ample funds and corresponding capability.

Ways of Increasing Counter-terrorist Capability

The countering of radiological terrorism needs to create capability at several parallel levels:

- Intelligence (technical, digital, and human);
- Prevention of terrorist and rogue elements from obtaining radiological and nuclear agents, or the equipment and know-how to produce them;
- The preparation of specialized teams to deal with radiological attacks in the field, even in urban warfare;
- Investments in R&D for detection, protection, decontamination, and treatment equipment and supplies;
- International cooperation in the fields of international law enforcement treaties, as well as in operational intelligence and monitoring of suspected nuclear, biological, and chemical terrorists.

The threat of large-scale acts of nuclear terror and the potential for radiological terrorism will enhance the need to prevent terrorist schemes and give warning before such acts happen. The utmost importance of early warning appeared clearly after the September 11 attacks in the U.S.; the U.S. Department of Energy was not at all prepared to deal with the use of hijacked civil aircraft for suicide attacks on nuclear power plants inside the country. In cases of nuclear terrorism without warning, even the first-responder teams could be destroyed before they act. In cases of radiological threat, the early warning could at least permit mobilization for counter-terrorism actions on the part of the endangered population. Therefore, it is important to develop a list of alert indicators concerning the imminent use of radiological/nuclear agents. Now e-indicators are in fashion in the U.S., but not yet in poorly Internet-equipped Russia.

The existence of small groups and cells of highly motivated religious extremists, left/right-wing fanatics, and unpredictable esoteric or millenarian cults—which in many senses act anarchically—means that the work of penetrating and infiltrating these groups is highly difficult. Thus the use of human sources of intelligence should be expanded and perfected; the counter-terrorism expertise, the cultural knowledge, and the language aptitudes of intelligence officers should be improved in military and civilian colleges and universities.

It is also important that intelligence services cover the so-called "gray zones" and do not permit the formation of blind spots in the overall intelligence picture, such as Afghanistan until recently, Somalia, some other areas in Africa, the jungles in the Philippines or Indonesia, etc. Such gaps in intelligence coverage would permit terrorist groups to find safe haven in such places in which they could grow, later to proliferate to the outside world. This means that the investments of governments in counter-terrorism capabilities, both human and technological, must be enhanced on a very large scale.

As far as the proliferation of non-conventional agents and weapons is concerned, particularly to the extent that it may impact terrorism and affect the security of whole countries, the coming decade will certainly present the most formidable task. The challenge in this case is two-fold: on the one hand, it is necessary to penetrate and monitor the activities of the various networks and organizations in their attempts to acquire or use radiological and nuclear material to create "dirty bombs" and other kinds of weapons to be used in asymmetrical warfare. On the other hand, there is a need to identify, monitor, and neutralize the providers of fissile material and nuclear and other technology and know-how used in the preparation of such weapons.

These counter-terrorism units' mission is linked to the overall task of preventing the proliferation of weapons of mass destruction to rogue states, but in many senses it is more intricate. This means that the interaction and cooperation between the security and military establishments, the scientific community, and industry must be strengthened and developed in a manner that can help identify at the earliest possible stage any interest shown on the part of rogue (non-state) elements in the search for non-conventional capabilities, radiological or otherwise.

Special attention should be given to the poor standards of security at nuclear facilities and the possibility that former—or even currently active—nuclear scientists and technicians would assist terrorist organizations in achieving nuclear/radiological capability (as the father of the Islamic nuclear bomb Abdul Kadir Khan in Pakistan did in favor of some rogue states, like Libya, Iran, and North Korea).

Nuclear waste facilities and transportation routes in the industrial countries should be also considered as potential sources of raw material for terrorist organizations, or as targets for attacks by these same organizations. This is even more true in many poor countries, which have become receptacles of such waste for economic reasons. Therefore, strict security measures must be adopted for these plants, deposit places, and transportation routes, above and beyond the IAEA requirements.

Particularly noteworthy is the case of two Pakistani nuclear scientists who in 2003 probably advised Osama bin Laden in his efforts to develop some kind of nuclear or

radiological capability. It is not yet clear how much they knew about the practical steps in this enterprise, and how much practical know-how they passed on to Al Qaeda. According to recent publications, hundreds of small radioactive power generators scattered across the Soviet Union decades ago and largely forgotten (a so-called problem of radiological "orphans"), could fall into the hands of terrorists. The IAEA's Illicit Trafficking Database includes over 280 confirmed incidents since 1993 involving radioactive sources. The actual number of cases may well be significantly larger than the number reported to the IAEA. Customs officials, border guards, and police forces continue to detect numerous attempts to smuggle and sell stolen sources.

There have been formed twelve international instruments related to the prevention and suppression of global terrorism, including the Convention on the Physical Protection of Nuclear Material. Ongoing efforts aim at the protection of nuclear material in domestic use, storage, and transport. Also on the list is the International Convention on the Suppression of Terrorist Bombings, which establishes as an offense the delivery or construction of a weapon or device through which there is a release, dissemination, or impact of radiation or radioactive material. The Non-Proliferation Treaty is also recognized for its contributions to nuclear security, which are no longer satisfactory under the growing pressure of radiological terrorism.

On the other hand, it should be noted that Russia has created a special elite force to defend its nuclear facilities and bases, and it seems that the level of security at these installations has greatly improved. Will the Kremlin wish to apply such experience to other CIS countries? There are doubts on this account, because of the lack of any draft of a counter-terrorism doctrine.

Another area of concern in building the counter-terrorism capability in Russia is the interest that criminal elements and organized crime syndicates show in this lucrative activity, although it must be stressed that, up to now, most of the known cases of smuggling of radiological materials have been either deceitful operations by swindlers or sting operations by Russian special and security services. Nevertheless, the activities of criminal elements in nuclear trafficking poses a great challenge to the established security system, as it is known that the connections between organized crime and terrorist organizations are difficult to monitor.

The funding of such illicit transactions, which involve great sums, implies the necessity for strict monitoring of financial transactions and money laundering. The measures taken in this regard by the U.S., Europe, and other countries as a consequence of the September 11 attacks illustrate the importance of this aspect of counter-terrorist activity. Lately it was learned that several large Muslim charity organizations in the U.S., which had been connected to Osama bin Laden for years, had contacts with terrorist operatives who tried to obtain radiological weapons for Al–Qaeda.

And, last but not least, the problem of cultivating a counter-terrorism capability with popular support is that these counter-terrorist measures could imply limitations on civil rights and liberties and on the right of the public to information. Let me show several examples of so-called "passive" preventive measures:

- The need to monitor the academic curriculum and the personal background of nu-

clear students and researchers involved in projects who may use their knowledge for illicit or violent activities (this would cover a pretty long list of nuclear sabotage cases at several nuclear power plants in the United States).

- There is already a trend to limit and censor the amount of open scientific and security information accessible on the Internet (the U.S. has decided to limit the data published on nuclear facilities, etc). Recently, there has been another initiative to get U.S. Congress approval for e-mail and web site monitoring of data connected to nuclear/radiological know-how, and even direct links to professional sites and e-forums that deal with such knowledge.
- Countries producing dual-use radiological materials will have to enact strict laws concerning the commercialization of these products in order to find the most efficient ways to monitor and ensure their proper implementation.

Finally, it is a commonly accepted idea that the physical and digital security of sensitive civil nuclear facilities, plants, and radiological laboratories should be greatly improved, and that access should be curtailed. Lately, the United States, Russia (in and around the Rostov nuclear power plant near Volgodonsk-city), and some European states have taken even military steps in order to defend such facilities, mainly nuclear power plants, in light of growing information indicating the interest of or plans by Islamist groups to attack them.

The U.S. has been the most advanced country in the preparation of the necessary emergency infrastructure to cope with the aftermath of a nuclear terrorist attack. The Defense against Weapons of Mass Destruction Act has permitted training in radiological preparedness for personnel in 120 major cities across the U.S., and this number has recently been increased to 157 cities. This includes training of emergency responders and medical personnel, virtual and field exercises in dealing with nuclear/radiological threats in cities across the United States, and the improvement in the planning and coordination of federal, state, and local agencies dealing with nuclear/radiological terrorism.

The U.S. has also developed training publications, technical reports, and planning guides, and has established some rapid response teams against signs of radiological terrorism, including its emergency communications system. In fact, the United States created such anti-terrorists units in the 1970s. There was the NEST (Nuclear Emergency Search Team), which from 1975 to 1993 intervened some thirty times in nuclear-related incidents. But none of these efforts were directed against non-state actors, and were dependent on numerous legal formalities.

Under the current Bush Administration, the U.S. is ready to enlarge its market of counter-terrorism "goods and services" in many countries. First of all, this undeclared counter-terrorism doctrine and corresponding capability are available to the few countries that can invest, even proportionally, the same financial, scientific, and technological resources in the defense against this and other kinds of non-conventional terrorist threats. Therefore, there is need for Russia, as well as the U.S., to help and support other poorly prepared countries to protect themselves in advance.

The Office of the Coordinator for Counter-Terrorism (S/CT) of the U.S. State De-

partment has already begun to do this: it trains host nations with American diplomatic and military facilities in a preparedness program for dealing with radiological and similar attacks, and offers first-responder awareness training. The S/CT also manages the interagency Foreign Emergency Support Team (FEST), designed to provide support to the host nation in the event of an attack on a U.S. installation in that country. This kind of assistance could be expanded to permit threatened countries to better prepare themselves for any attack, even one not connected with U.S. or Russian nuclear interests.

It is an accepted axiom today that cooperation on the bilateral, regional, and international levels is essential in preventing and neutralizing global terrorism. Without sincere and close cooperation between the various countries in the intelligence field, each country, as past experience has shown, will at some point become a victim of terrorism, including in its radiological forms.

A promising development in 2004 was the creation of the Terrorism Prevention Branch (TPB) of the United Nations, under the rubric of the Center for International Crime Prevention. The TPB intends to research the subject of WMD terrorism and develop a set of practical advisories to UN member states to cope with the threat. There have also been initiatives on the part of countries like France and Russia to improve international legislation at the United Nations concerning the financing of terrorism or the prevention of nuclear terrorism. The advanced industrial countries—not only the G-8 countries, but also Singapore, China, India, South Korea, Brazil, and others—are to invest and participate in a coordinated international effort to develop technical prevention tools, because in the long run every country could be a target for nuclear/radiological attack or blackmail.

Traditional international arms control measures are less effective in monitoring and controlling proliferation efforts by small terrorist groups, and might not detect the development of a radiological dispersal device or other tools of radiological terrorists, who may easily use legal commercial supplies and equipment, to say nothing of illegal ones. Nevertheless, traditional arms control measures may influence behavior, though they will be more effective when directed at state sponsors of terrorism, slightly touching non-state actors in the process. However, it is important to build international consensus against radiological terrorism, not only for the sake of prevention or the simple isolation of small states from nuclear energy projects (which is counterproductive for nuclear energy in its historic competition with fossil fuels), but for quick liquidation of radiological terrorism advocates as combatants in asymmetrical warfare. They are no longer "criminals" who deserve trials and imprisonment.

Counter-Terrorism Doctrine: From Intelligence Gathering and Exchanging to Surgical Strikes without Trials

In August 2001, President Bush received a two-page report on Al Qaeda's intentions to attack U.S. vital interests in the coming months. There were no signs of terrorists' practical steps inside the U.S. that could be disrupted beforehand. Of course, good intelligence is the best weapon against terrorism. While reactive investigation may prove useful for some purposes, now it is generally considered that, with unpredictable

crimes like terrorism, a proactive strategy is best. When in reactive mode, there is a tendency to throw the full range of resources at the problem. This is not necessary, because terrorists do have quite predictable social and psychological motivations.

In many ways, terrorists simply behave like common criminals who take politics and religion very seriously. Also, because they have no legitimate social structure (like a nation-state or official organization) supporting them, the role of group support and the group's belief system becomes extremely important. At a minimum, Russia-NATO analysts must strive toward including all the following in intelligence gathering and interpretation:

1. *Group Information*: Name(s), ideology (political or social philosophy), history of the group, dates significant to the group, and dates on which former leaders have been killed or imprisoned. (Terrorist groups often strike on important anniversary dates.) Some groups also have a scripture or manifesto, which is important to obtain (doomsday dates). So it is clear that "soldiers of Allah" are not the only ones born with a death wish, but are created by specific conditioning processes of indoctrination, recruitment, and training. And they are not to be treated as criminals and future POWs, because they are happy to sacrifice their life.
2. *Financial Information*: Source of funds, proceedings from criminal activities, bank account information. For example, sudden influxes of funding or bank withdrawals indicate preparation for activity. It is also important to determine the group's legal and financial supporters. Generally, anyone who would write an official letter of protest or gather names on a petition for a terrorist is a legal-financial supporter. Sometimes, an analysis of support may reveal linkages and/or mergers with other domestic and/or foreign terrorist groups.
3. *Personnel Data*: Lists of leaders (and changes in leadership), lists of members (and former members), any personal connections between its members and other groups of similar ideology, and the skills of all group members (in this case, nuclear weapons expertise, electronics expertise, etc.) Knowing the skills of the group is an important part of threat assessment. If the philosophy revolves around one leader, it is important to know what will occur if something happens to that leader. Often, the analysis of family background is useful to determine how radically a leader or member was raised. Group structure, particularly if the organization pattern is cellular, determines who knows whom.
4. *Location Data*: Location of group's headquarters, location of group's "safe havens" (where they hide from authorities), and location of group's caches (where one may hide fissile materials and other components of nuclear weapons and supplies). Out-of-the-blue attacks on caches are the most fruitfully used counter-terrorism technique. It is important to specify the underground that exists where terrorists can flee. This is harder than detecting safe havens. Terrorists like to live in communal homes instead of living alone. These civilians may become victims of radiation from hidden fissile materials, even in small quantities. That is why human intelligence is of such great importance.

Today's radiological terrorists defy deterrence or suppression because they do not seek targets of opportunity as ordinary criminals do, but rather focus on symbolic targets. As a group, terrorists are very team-oriented, and always prepared for suicide missions. Average criminals are undisciplined, untrained, and oriented toward escape. Terrorists are just the opposite. They have prepared for their mission, are willing to take risks, and are attack-oriented. If captured, they will not confess or snitch on others, as ordinary criminals do. Traditional law enforcement methods of investigation are not all that effective in obtaining useful information about terrorism, and terrorists cannot be deterred like ordinary criminals and treated as POWs. They should be attacked with deadly surgical strikes, without any need for trials or investigation, if there exists digitally proved evidence of their fatal intentions. Supercomputers equipped with smart software cannot be mistaken in such a judgment. And it does not matter that operators of these analytical devices may have the chance to promote the counter-values of totalitarianism.

Response Requirements

Authorities in all IAEA member states need to incorporate the above mentioned responsibilities into legislation, plans, and procedures in order to minimize the probability and the consequences of such events. It is also recognized that all NATO countries and members of the European Union are increasingly dependent upon each other. So, any misconduct in one NATO or EU country may end up as a nuclear emergency or radiological accident in another nation, requiring a well-coordinated response there. It is therefore essential that the security of radioactive sources and the response to radiological emergencies not be considered just as a national problem. They need to be addressed on the regional and global level, and treated as problems that have to be solved through newly formed modalities of international cooperation, with an emphasis on counter-terrorism against non-state actors.

In responding to radiological emergencies of any kind, it is recognized that:

- It is the responsibility of authorities in the respective states to respond;
- Handling these events may require tools such as combat units representing several states;
- Handling these events in a state that harbors terrorists may require resources exceeding the capabilities of several counter-terrorist units.

In order to be able to fulfill their tasks, these units need real time information from the national or international center of counter-terrorism, and financial and material resources (both state and private). In order to be able to respond to emergencies or potential emergencies in the best possible way, any counter-terrorist unit should establish mechanisms of cooperation in line with the recommended vision of the common doctrine of counter-terrorism.

There are formal interstate regulations that will need to be revised. The IAEA member states need to review the legal framework and propose ways of improving the cooperation mechanisms so as to ensure more binding commitments from member states to provide adequate and timely information to other member states at any sign of

a radiological threat or nuclear event. Such an international scale for response to nuclear events has been developed; what is needed is a more detailed scale for mini-threats of a radiological nature.

Moreover, there could be developed UN special service approaches on the basis of this preemption concept of counter-terrorism. But no concept can be approved without first testing existing counter-terrorism technologies. So one should clearly recognize that enhancing the mechanisms of international cooperation in response to nuclear and radiological terrorism and similar emergencies would be significantly reliant upon the UN member states' military capabilities for responding to such emergencies and making such responses more cost efficient.

For example, the IAEA member states could follow up on IAEA General Conference Resolution GC (46)/RES/9 and enhance their efforts to improve their national nuclear and radiological security capabilities, implementing international standards and recommendations. The same mechanism is quite adaptable to international cooperation in counter-terrorism in response to small-scale radiological emergencies.

Common Counter-Terrorism Measures

In the early 2000s, passive measures of anti-terrorism were in widespread use. For example, in Turkey people used to call a three-digit telephone number operating around the clock if they found any radiological materials. All companies that were involved in nuclear/radiological industries had to have their personnel trained on-site and then be certified by the Turkish Atomic Energy Authority.

Around the world there are many online educational programs and training seminars with a focus on preparedness for and response to radiological accidents that have already happened. After such e-certification, nuclear regulatory commissions in the IAEA member states urge staff to prepare emergency response plans.

In Spain, some planning is in place for nuclear power plants, but emergency preparedness for dealing with radioactive sources is less structured. An emergency plan should include a reference hospital, which nuclear regulatory authorities have in Madrid. Any radiation victim might be immediately transferred there by helicopter. But the Spanish plan deals with a nuclear accident for which there was some warning, not an unexpected mini-attack by radiological terrorists.

I suggest a benchmarking study with the aim of compiling a practical list of best practices within Russia and NATO. Then, such a research team may form a corresponding database for the IAEA, the new counter-terrorism bodies of the UN, and the general public. It will have a deterrent effect on terrorists, and also maintain civilian resistance to their mini-radiological threats.

We need an Internet-based checklist of any attempts at radiological terrorism in the world, updated and accessible around the clock, seven days a week. While it is absolutely clear that certain response actions are needed for an emergency situation arising from a radiological dispersal device, we also need to prepare for what precedes that event. For instance, what is to be done when we have a report of the theft, or when we know that something is on the move to a store of radiological materials? This is a new, challenging situation, which requires further analysis and, more importantly, action.

Recently, nuclear nations have begun to focus on the small number of countries bent on violating the nuclear non-proliferation norm and acquiring fissile materials for nuclear weapons. But the radiological materials that could be used in "dirty bombs" exist in a variety of forms in virtually every country in the world. And they are often only loosely monitored and secured, if at all. Taking measures to control dangerous and vulnerable radioactive sources is the responsibility not just of a few nations, but of all nations. That is a new job for their national security systems.

Last year, the United States announced the Radiological Security Partnership Initiative. It is a three-pronged approach to addressing the potential threats from under-secured, high-risk radioactive sources. The first prong is helping countries accelerate and expand national initiatives to keep track of and better secure national inventories of high-risk radioactive sources. In this regard, the new U.S.-Russia partnership may include another new initiative to provide some technical assistance and equipment to Russia-NATO Committee member states to facilitate effective tracking of high-risk sources. Second, all countries need to draw on international re-training resources that can give practical advice and assistance in bringing these radiological sources under tighter control. The Russian Federation is currently working with the U.S. and the IAEA to identify and secure high-risk radioactive sources in the territories of the former Soviet Union. This tri-party model may be adapted to meet the counter-terrorist needs of other countries. Such a model is working well in the territories of the former Soviet Union, and could become global in scale.

Of course, there are some bottlenecks, like the budget convergence of the Russian Ministry of Defense and the Ministry of Industry and Energy through the Federal Agency of Nuclear Energy. All these budgets are quite opaque to foreign investors. Here is a good example provided by NATO countries: they have a lot of extra-budgetary support for military innovations as a result of their financial transparency for investors and sub-contractors. In Russia, unfortunately, financial transparency of the power ministries is a dream. But joint counter-terrorism measures require trust in order to work. The U.S. has established numerous detection checkpoints on suspected smuggling routes, in order to better detect illicit traffic in radioactive sources. And the same initiative is under way to improve the ability of Russia-NATO to detect the transport of radiological or/and nuclear materials into our countries from outside. As the third prong of this plan, I would now expand this project by focusing on other major transit and shipping hubs, which will improve joint Russia-NATO efforts to interdict and prevent illicit trafficking in high-risk radioactive sources globally.

There are some good results coming out of the IAEA consultations that are leading to approval of selling U.S. border monitoring equipment to many countries. This equipment in some cases can be as simple and small as the radiation pager in the form of a car-key trinket. Such small devices, when used in large quantities, can play a decisive role in the growing effectiveness of this critical global counter-terrorist initiative. By working with mobile telephones and through the Internet, such a Russia-NATO shared focus on reducing the potential threats from both the highest and most minimal radiological risk sources will bring excellent results. So human intelligence is to become the key element of the counter-terrorism strategy, but aided by technology.

The Radiological Security Partnership has already become a U.S. priority, but the contribution made—only $3 million over the next fiscal year—is a tepid demonstration of the Bush Administration's commitment to the Partnership. In particular, this money will support joint efforts to work with governments of developing countries to secure high-risk radioactive sources in their countries.[3]

Old, Useless, and Expensive Measures for Protecting Radiological Materials

Many analysts have come to two logical conclusions: first, the safety and security of radioactive sources are intrinsically linked one with the other; second, source security must be an important but subordinate element of source safety, not the other way around. The subsidiary nature of the security of radioactive sources with respect to their safety has been recognized over the years in both international and national standards dealing with radiation, where security requirements have ranked as important but not all-encompassing elements of safety standards. Thus, radiation safety is concerned with preventing adverse health and environmental impacts from radiation sources in general, and radioactive sources in particular.

Traditionally, radioactive source security has been looked at as concerning preventing the loss of control of the source, whether through inadvertent, intentional, or malicious means. Nowadays, it is better to direct some pre-emptive strikes at the fingers or hands of those who try to reach radioactive materials. It is no use to shoot the legs or chase previously established terrorists after lethal combat (not criminal!) operations. You may guard radioactive materials, and you may use preventive strikes on terrorists. The latter is cheaper and more effective.

Why should radioactive sources be the focus of security interest when hundreds of dangerous chemicals and biological agents are readily available for harmful terrorist acts? It is not evident that a radiological dispersal device could be an element of terror—its potential effects cannot be compared with the catastrophic consequences of a nuclear, chemical, or biological weapon—but the public does not necessarily perceive the difference. It is just as much a tool of blackmailing oil and gas lobbies against nuclear energy as a competitor in the global energy market.

The Russian-American Dream about Radiological Terrorism Prevention May Come True

At present, the counter-terrorism capabilities of Russia and the United States are completely incompatible. See the U.S. structure, as follows:

- The Terrorist Threat Integration Center (TTIC) and the Terrorist Screening Center (TSC) were both created with full support of the U.S. lawmakers as a response to the U.S. intelligence failures prior to the September 11 attacks. The TSC was opened in December 2003 to consolidate all the U.S. government's terrorist watch lists into one central database.

[3] See D. Huizenga, "Key United States Programmes for the Security of Radioactive Sources, in *Security of Radioactive Sources*, proceedings of an international conference held in Vienna, Austria, 10–13 March 2003, 85–94.

- The TTIC, which began operations almost two years ago (in May 2003), serves as the U.S. federal government's hub for terrorism-related analysis. It collects information from all fifteen U.S. intelligence agencies.
- The joint efforts of these centers, with information flowing back and forth between them, create the daily threat matrix for the president.

In Russia, on the contrary, there is lack of cooperation between even departments within ministries and federal agencies, to say nothing about private businesses, like in the U.S. At this point, no official counter-terrorism doctrine has been developed for the Russian Federal Assembly to be adopted as a set of laws to make counter-measures legal and transparent to public scrutiny. But steps in this direction are to be made.

The number of terrorist elements is not large. But this does not mean that the new counter-terrorism preparations and legislative steps are unnecessary. On the contrary, in Russia and other NATO countries, we are already witnessing some groups, particularly those engaged in the collection of funds for terrorist organizations, retreating. In addition, we have seen non-Russian individuals—hard-core members of various nationalistic and separatist groups—who are now willing to talk to us and, in some cases, to assist counter-terrorist units.

To this end, the Russian counter-terrorism capability can be described as follows:

- Efforts of Russian and NATO law enforcement agencies to track down terrorist activities as counter-terrorists pursue their investigations;
- Devoting greater effort to providing information on screening procedures for governments of the G-8 countries as leaders in nuclear energy development, including their corresponding ministries of defense, energy, labor, citizenship and immigration, and finance;
- Pursuing its own preventive investigations, particularly those on domestic and foreign extremists, in order to be able to provide intelligence about possible future attacks.

On the wider front, Russia, along with other Western democracies and their Asian analogues in Central Asia, has already introduced many anti-terrorist legislation initiatives (the Shanghai Six Countries Agreement). Many Russian anti-terrorism acts have already created the capability to deter, disable, identify, and prosecute those engaged in terrorist activities or in supporting these activities. The intent of the legislation makes it an offense to knowingly support terrorist organizations, whether through overt violence, or by providing support through documentation, shelter, or funds. One integral part of the new Counter-Terrorism Capability Act requires e-publication of a list of groups in the world deemed to constitute a threat to the security of Russia and NATO.

Before the events of September 11, the G-7 and Russia (G-8) preferred to discuss ways of combating terrorism. For example, in the Ottawa Declaration of 1995 there is a set of "guidelines for action" intended to increase international collaboration in the prevention of terrorism that committed member countries to:

- Refuse substantial concessions to hostage-takers, ensure those responsible are brought to justice, and join existing international treaties on terrorism by the year

2000;

- Promote enhanced mutual assistance of a legal nature;
- Pursue measures to prevent the terrorist use of nuclear, chemical, and biological materials;
- Inhibit the movement of terrorists and falsification of documents;
- Strengthen counter-terrorism cooperation in maritime, air, and other transportation sectors;
- Counter terrorist attacks against public facilities and infrastructure;
- Deprive terrorists of funds;
- Increase counter-terrorism training.

Russia declared its full support for United Nations Security Council resolution 1373, adopted by the Security Council on 28 September 2001, aimed at international terrorism. In the future, persons knowingly providing support for terrorism, whether through overt support, or by providing funds, materiel, or shelter, will be deemed criminals. But, in fact, they are combatants, who are deserving of pre-emptive strikes (before they are able to reach radiological weaponry, for example), instead of legal procedures in courts "after capture" if their "dirty bomb" did not work.

Meeting for the first time since the tragic events of September 2001, the leaders attending the June 2002 G-8 Summit in Kananaskis, Alberta discussed many challenges and new tasks in fighting terrorism. Russia confirmed its commitment to reduce the threat of terrorist attacks, but no counter-terrorism doctrine has been developed and approved at the federal level at this point. All corresponding decisions have been made at ministerial levels, with meager results in maintaining counter-terrorism capability. In the recently formed Federal Agency on Nuclear Energy (the former Minatom), for example, the threat of radiological terrorism is considered to be "exaggerated."

Why is this so? In Russia and other NATO countries, there are fears that a more robust counter-terrorism capability will foster Russian, American, Canadian, etc. versions of the Gestapo, or will stimulate political repressions against legal opposition.

At any rate, in 2002–4, Russia and its G-8 partners agreed on a set of six non-proliferation principles aimed at preventing radiological terrorists (or those who harbor them) from acquiring or developing nuclear and radiological weapons, missiles, and related materials, equipment, or technologies.

Russia, like other CIS countries, has a UN mandate to collect information both at home and abroad, and to advise NATO countries' governments about activities that may constitute a nuclear/radiological threat to the security of the Russian Federation. This includes any NGO or even anyone who advocates the use of radiological threats as a tool of violence to further political, religious, or ideological objectives. In the 1990s, when Russia was engaged in wars in Chechnya and other "hot spots," the ratio of operational anti-terrorist resources devoted to the military, interior forces, and Federal Security Service's counter-terrorism and counter-intelligence programs was approximately 80 percent to 20 percent in favor of counter-terrorism. Under the first and the second terms of President Vladimir Putin, this ratio has now tilted substantially in

favor of counter-intelligence, making public safety—the protection of Russian lives—no longer the number one priority of Russia.

Conclusion

Dealing with problems that are more distant and more foreign requires better understanding and communication. Common threat assessments are the best basis for common actions. This requires improved sharing of intelligence among member states of the IAEA, and with Russian partners in the enlarged NATO. Which form of cooperation will be the best will be seen in the near future.

As we increase our capabilities in different areas of counter-terrorism, we should think in terms of a wider spectrum of missions. This might include joint disarmament operations, support for third countries in combating terrorism, and security sector reform. The latter would be part of a broader process of institution building. Some skeptics even were promoting postponing last year's presidential election in the United States, if the Bush Administration was late in forming a proper counter-terrorism capability. There were some historic precedents for this, such as when Franklin Roosevelt was re-elected several times under pretexts of preparations for the World War actions against the Axis powers.

Now the European Union is reluctant to strengthen its counter-terrorism capacity because of a different political situation. Russia also is not in any hurry, because topics of terrorism prevention already helped President Putin's team in the recent re-election in March 2004. Now this team feels no need to devote extra resources to counter-terrorism measures, although a lot of rhetoric is in the air. On the whole, European countries and Canada are not taking active steps in this direction. Their previous concept of joint anti-terrorism security has been worked out inside the old NATO structures. And all the innovations that the U.S. is promoting seem to them expensive and even counterproductive.

However, it has been recognized that potential "dirty bombs" disrupt society by creating public panic based on fear of radiation, and they also create a zone where significant cleanup efforts must be undertaken at potentially great cost. Thus, there is sort of an Euro-Atlantic security "doctor's dilemma": to foster radiological terrorism fears among citizens in order to make them ready to "swallow" counter-terrorism measures (including, for example, such a "remedy" as cancellation of presidential elections); or, vice versa, to continue to ignore "futile" fears in the face of growing radiological threats, like Russia and some European Union countries do. Such a position may dismiss any pre-emptive measures against global terrorism, including radiological threats, instead emphasizing traditional anti-terrorism methods.

Today, small and unstable countries like Myanmar or Syria are on the way to a "nuclear future." If the counter-terrorism doctrine is approved by the UN Security Council, and Russia-NATO teams are given corresponding license to prevent radiological terrorism, this nuclear future will be far safer than the nuclear present. It means that the global functions of the enlarged NATO will not create "conflicts of interests" between nuclear nations and states of the so-called radiological "gray zone," through which poorly monitored transportation of radiological materials occurs.