G8 INITIATIVE FOR PUBLIC-PRIVATE PARTNERSHIPS TO COUNTER TERRORISM

Private Sector Action Beyond 2006
EWI's DISCUSSION PAPER

November 2006

Executive Summary

In November 2006, Russia will host the Global Forum for Partnerships between States and Businesses to Counter Terrorism. This event marks the completion of a successful year of international mobilization by Russia as President of the G8. The decision by the G8 countries in St. Petersburg in July of 2006 to support the Russian initiative in this field has been one of the most important decisions in the field of counter-terrorism in a long time. This decision gives further impetus to a number of pre-existing moves in the direction of establishing public-private partnerships to combat terrorism.

Through 2006, Russia led a series of preparatory meetings and related events in major capitals (London, Paris, Berlin, Brussels, Washington and Moscow) involving more than 600 representatives of government and business. These events confirmed that leaders in both government and business have recognized the concrete potential of this initiative. Propositions have been received in areas ranging from cyber security and financial services to the protection of critical energy infrastructure. Russian companies have been extremely active in the process. G8 leadership in this area of public-private partnerships for counter terrorism has been and will remain important. To ensure concrete advances in the specific areas noted for action continued leadership by the Russian government, while working within the framework of the G8 is essential.

All parties now face a choice in defining effective frameworks to take this initiative forward. The Moscow Strategy, a declaration of strategic intent to cooperate in this area, launches the process. It will be a centerpiece of the event in November and the foundation for subsequent development. A number of concrete proposals for further work in this area will also be discussed at the November meeting. The meeting is expected to support the continuation of the Russian initiative and its further development in concrete areas, through two tracks.

The first track will be an annual international conference with broad G8 and other international representation.

The second track will be the creation of small industry-specific or issue-specific "Working Groups" (such as cyber security). These groups will proceed at the initiative of the private sector working with governments to facilitate either the rapid acceptance by government of emerging technologies from the private sector or more effective communication between government and businesses of different nationalities on mutual needs for effective and economically viable responses to terrorist attacks or to the effects of terrorist attacks.

TABLE OF CONTENTS

Introduction

Following the G8 initiative on S*trengthening Partnerships between Governments and Businesses to Counter Terrorism* presented at the Worldwide Security Conference, co-organized with the EastWest Institute, a series of preparatory meetings were held in Berlin in June of 2006 and Brussels in July of 2006 to discuss how to improve cooperation between governments and businesses in the fight against terrorism. Other events were held in London, Paris, Berlin, Brussels, and Washington. An international conference of more than 300 people convened in Moscow on October 11. In November 2006, Russia will host the Global Forum for Partnerships between Governments and Businesses to Counter Terrorism. This event marks the successful completion of Russia's Presidency of the G8 in 2006 and international mobilization on this important topic. The Forum is expected to endorse the "Strategy for Partnerships between States and Businesses to Counter Terrorism" (hereinafter called the Moscow Strategy), a document drafted by the G8 in consultations with private sector leaders during the course of Russia's G8 Presidency.

This paper represents a compilation of feedback and reactions from the business world and various governments arising from the series of meetings and considers possible ways ahead for business in responding to the Russian initiative beyond 2006.

G8 Summit Declaration on Counter-Terrorism

At the G8 Summit in St Petersburg in July 2006, the heads of state endorsed a Russian initiative to promote better collaboration nationally and globally between governments and the private sector in the fight against terrorism. The endorsement came in the form of the St. Petersburg Summit Declaration on Counter-Terrorism issued on July 16, 2006.

The statement recognizes the UN as having the central role in the coordination of the fight against terrorism, and the G8 members committed themselves to supporting and strengthening the UN's efforts in this area. Secondly, the G8 members recognized the urgency of enhancing cooperation to prevent or react to terrorist or other criminal attacks on critical energy infrastructure. Thirdly and perhaps most importantly, the members emphasized the importance of working with the private sector to counter terrorism and to protect private citizens and businesses.

The Declaration includes the following statement: *"We emphasize the importance in a globalized world of working closely with our private sector partners in our efforts to counter-terrorism and bolster capacity to protect our citizens and businesses as they pursue their work and leisure. We commend the 'Global Forum for Partnerships between Government and Businesses to Counter-Terrorism', to be held in Moscow in November 2006 and commit to close cooperation within the G8, with other States and with business partners to make this initiative a sustained and successful process."*

The United Nations Global Counter-Terrorism Strategy adopted by the UN General Assembly in September 2006 encouraged the United Nations *"to consider reaching out to the private sector for contributions to capacity-building programs, in particular in the areas of port, maritime and civil aviation security."* The G8 St. Petersburg Summit Declaration goes beyond this particular form of cooperation between governments and businesses, recognizing the latter as an essential global partner in many areas critical to preventing terrorism.

The Declaration identified a number of steps needed to enhance international efforts to combat terrorism. To some of these steps, businesses can contribute in an effective way. They include:

- Implementing and improving the international legal framework on counter terrorism.
- Ensuring that national legislation is modified to address new terrorist challenges.
- Suppressing attempts by terrorists to gain access to weapons and other means of mass destruction.
- Enhancing efforts to counter the financing of terrorism based on agreed standards.
- Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists.
- Promoting supply chain security, based on existing international standards and best practices.

This G8 initiative and the G8 Declaration were endorsed by Eurochambers, the Association of European Chambers of Commerce and Industry representing 17 million firms in the EU and Russia. Their report, issued in July 2006, called for special attention to the protection of critical infrastructure. It noted that in the US, as in Germany, 85 percent of critical infrastructure is in private hands. They took the view that prevention is the most important goal and noted that the private sector offers enormous potential in terms of innovative solutions and, in most cases, works with more flexibility and efficiency at lower costs than the public sector. When tasks and risks are redistributed properly, reducing the burden on the government and opening new markets for businesses can create a win-win situation. Without security, the economy cannot flourish.

Public Private Partnerships to Counter-Terrorism before 2006: A Slow Start

The use of public-private partnerships to counter terrorism is not a new concept but the record has been patchy to say the least. There have been doubts and suspicions on both sides in working toward practical measures, not to mention very real concerns in government circles about compromising the security of state operations. There has also been a lack of precision on what the appropriate form of cooperation might be, especially when more than one government needs to be involved. Indeed, international cooperation in counter-terrorism work involving only governments still faces many challenges. This section gives a brief overview of related developments before the St. Petersburg summit.

In May 2000, Japan's peak industry association, Keidanren, identified the importance of ensuring that information-security be enhanced in the face of terrorist threats. It said it was essential that government institutions and private corporations collaborate to devise countering measures targeted at hackers and cyber terrorists. For the sake of national security, Keidanren called for better cooperation among industry, academia and government in the area of research and development to increase the level of information-security.

In the United States, the 9/11 Commission reported in November 2003 that in order to prevent another catastrophe, major focus should be placed on partnerships -- partnerships between federal, state and all local levels of government, as well as between the public and private sector, and between civilian emergency responders and the military. With approximately 85 percent, if not more, of US critical infrastructure in private hands,

improved cooperation is vital, the Commission said.[1] It noted that interdependencies of the public and private sector are crucial in ensuring the security of the national workforce and infrastructure. The report identified three key areas for improving private sector cooperation:

1. Sharing information on private sector "targets."
2. Improving internal security measures.
3. Creating resilient and robust systems.

Other Multilateral Efforts in PPP to Counter Terrorism

The Asian Pacific Economic Cooperation (APEC) has also stressed how crucial public-private partnerships are in deterring terrorism. Public-private partnerships dominated the discussion at the Fourth Secure Trade in the APEC Region (STAR) Conference in February 2006. Participants, including Russian officials, urged that more partnerships at both the domestic and the inter-regional levels are needed. They emphasized that the private sector, including small and medium enterprises, should not be viewed simply as fund providers but as partners in implementing security measures and included in the decision-making process. "Government and industry must work together toward common goals," notes David L. Cunningham Jr., President of FedEx Express in Asia Pacific. "Securing and facilitating international trade flows is a long-term task that requires holistic and long-term thinking. Standards need to be harmonized globally." Information-sharing between the public and private sector "is critical in mitigating risks," adds Earl Agron, Vice President of Security at American President Lines, a subsidiary of Neptune Orient Lines, which is a global transportation and logistics company. "The private sector is going to be sharing more and more information with law enforcement and different countries will be sharing information amongst themselves. All of this requires trust among the parties involved."

Private Sector Leadership in Thwarting Nuclear Terrorism

Since a substantial portion of the nuclear infrastructure is controlled by private sector utilities, laboratories, or university research centers or institutes, it is the area of nuclear terrorism that offers a somewhat dramatic illustration of how important the G8 initiative is. There are two powerful examples of how effective public-private partnerships can be in preventing terrorism or in leading efforts: the Business Executives for National Security (BENS) and the Global Initiative to Combat Nuclear Terrorism.

BENS is self-described as "a nationwide, nonpartisan, member-driven organization working to help make America safe and secure." The organization is comprised of senior members and significant private sector firms. One of BENS' major achievements is the "Cooperative Threat Reduction Program." At an annual cost of just one-tenth of one percent of the defense budget, they have been able to deactivate thousands of nuclear warheads, destroy hundreds of missiles, bombers and submarines. Their objective is to remove the threat posed by the vast Cold War arsenal of the Soviet Union, which might fall into terrorist hands. There is still a

[1] US legislation defines critical infrastructures as 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters'.

significant amount of work to be done and much more remains to accomplish in terms of securing nuclear weapons and destroying millions of deadly chemical arms.[2]

The Global Initiative to Combat Nuclear Terrorism, though coinciding with the Russian G8 initiative for private-public partnerships to counter terrorism, provides another strong example of the powerful contribution the private sector can make. It is a joint initiative of Russia and the US. The central objective of the Global Initiative is to establish a growing network of partner states and private sector firms that are committed to taking effective measures to build a layered defense-in-depth that can continuously adapt to the changing nature of the threat. The approach begins with protecting nuclear materials at the source. Here, the Global Initiative will build on activities underway through the Cooperative Threat Reduction (CTR) and International Counter-proliferation Programs and other nonproliferation assistance programs. The goal is to stimulate partner states to invest greater resources in their own capabilities to protect nuclear materials on their territories. The Global Initiative includes detecting nuclear materials entering ports and urban areas, and sharing best practices with foreign port operators; preventing the sabotage of ships carrying nuclear materials, and stanching the flow of funds to terrorists seeking to buy nuclear materials on the black market.

Threats to Energy Infrastructure

Another area of concern is the possibility of terrorist attacks on energy infrastructure, which is somewhat linked with cyber-security. On February 24, 2005, an attempted suicide bombing of Saudi Arabia's Abqaiq oil facility, the largest in the country, was thwarted. Had the attack been successful, global oil prices would have increased to over $100 a barrel. John Chamberlain, (Security Manager, Asset Protection Services Corporate Security, Shell Oil Company) testified before a Congressional Committee on July 27, 2005 that after 9/11 Shell partnered with federal and local authorities to reevaluate and strengthen domestic security. Nationwide, oil and gas companies made major investments in strengthening facility-protection, offering extensive training and improving communications from wellheads and offshore platforms to tankers, ports pipelines, refineries, storage tanks and, most importantly, employees, contractors and key communities. He went on to state, "all these steps were carried out in close partnership with federal, state and local law enforcement, and security officials. The partnership forged between the oil and natural gas industry, and governments at all levels is now helping protect hundreds of facilities across the country from the possibility of terrorist attacks." Furthermore he stated, "a terrorist, unlike a pollutant or physical workplace environment, is clever and has the ability to adapt against a checklist of rules. This is one reason we value our close, professional partnerships with government, industry and local communities."

[2] In May of 2005, BENS successfully backed full funding for CTR. In July, BENS President Chuck Boyd and Chairman Stanley Weiss, writing to all 100 senators, called for passage of an amendment to lift red-tape restrictions hobbling CTR; the Senate agreed, by an overwhelming, bipartisan 78-19 margin. In a subsequent opinion piece in the *Washington Times*, Weiss and BENS member Ted Turner again urged the full Congress to approve the measure. The final result was a good one - Congress agreed to fund CTR's 2006 operations to the tune of $416 million and a permanent waiver of those red-tape restrictions.

Threats to Transportation

Aviation security has been one of the highest priority-issues in countering terrorism for more than 30 years. Since December 2003, Australian airline Qantas has been paying for Sky Marshals who are trained by the Australian Federal Police to sit on flights. Qantas provides training and equipment for security assistance to ground handling agents and local security services at airports in Indonesia, the Philippines and India. At $250 million last year, the airline's spending on security is larger than the budgets of some of Australia's state police forces. The funds went not only to paying the sky marshals, but also to implementing 100 percent checked bag screening at all major airports, and airside access controls, which can inspect or search all personnel moving to the airside of airports.

Another example of a public-private partnership that is being used in the area of transportation is the partnership between the Canadian Air Transport Security Authority (CATSA) and the private sector to develop a Restricted Area Identification Card, which utilizes cutting edge biometric technology. The addition of biometrics, along with centralized databanks, allows for the positive identification of the cardholder, and provides the ability to track, in real time, the issuance, verification and cancellation of passes. To date, 30,000 airport workers at nine of Canada's major airports are enrolled in the program. Once enrollment is complete, 120,000 airport workers will be registered at 29 airports.

FedEx is also actively involved with governments around the region on initiatives to increase trade and security. It is one of 31 associations and companies in the Private Sector Consultative Group working with the World Customs Organization (WCO) in Brussels to draft the details for a global framework of standards for security and trade facilitation - the SAFE Framework. It is also a member of C-TPAT (Customs-Trade Partnership Against Terrorism). In partnership with the private sector, the Customs-Trade Partnership Against Terrorism is a program managed by the US Department of Homeland Security, which aims at trying to secure the entire logistics chain. C-TPAT requires cooperation by government, importers, carriers, brokers, warehouse operators and exporting manufacturers. Qualifying to become a member of C-TPAT is a collaborative effort. Once C-TPAT certified, a company eventually goes through a validation exercise with Customs. For this validation, the C-TPAT representative from the private company and one or two C-TPAT Supply Chain Specialists will do a site investigation and review the security practices in place.

GE Homeland Protection has been working with the public sector in several countries to deploy new security solutions in the aviation sector, in particular through the introduction of Computer Tomography Technology for checked bag screening. A good example of a successful public-private initiative is the so-called “Registered Traveler Program,” developed with the US Transportation Security Administration. The program combines detection technology with biometric screening of the traveler into a single ID Kiosk. It was developed to provide expedited security screening for passengers who volunteer biometric and biographic information to a TSA-approved Registered Traveler vendor and successfully complete a security threat assessment.

The Container Security Initiative (CSI), which involves the posting of US Customs officials at major ports in order to pre-screen cargo destined for the US, is another area where the public and private sector must cooperate. American customs officials do not have the authority to inspect cargo, relying instead on their counterparts from each host economy to undertake physical checks. “You cannot have an Achilles heel anywhere in the system - if

you have 10 ports and nine of them are very well-equipped and the staff is well trained with regards to technology and you have one that is the weak link, then the whole system falls down because the terrorists will definitely exploit the weak link," says Gordon Chu, Co-chair of the Trade Investment Facilitation Working Group within APEC's Business Advisory Council.

General Electric has successfully partnered with government to address the management of energy resources and maintaining security against the spread of terrorism. "GE has invested millions of dollars to develop technologies that expand the tools available to government - often in partnership with the private sector." An example of such technologies is the "container-security device" that can detect and report unauthorized intrusions into oceangoing containers in order to help prevent the introduction of weapons of mass destruction into international commerce. The resulting product, the Commerce Guard is the first global, cost efficient system that deters and detects theft, smuggling and international terrorism by integrating electronic container security devices with a global information network. Starbucks recently became the first commercial purchaser of Commerce Guard and will install the technology on shipments of coffee beans originating in Guatemala, bound for the US and Europe."

Threats to Cyber-Security

Another key area of concern is information technology. In May 2004, the Business Roundtable called on software producers and end-users to join together in building a more unified defense against the increasing number, and growing cost, of malicious attacks on the global digital network. Michael Armstrong, Chairman of Comcast and Chairman of the Roundtable's Security Taskforce stated, "The interdependence of cyberspace means the attacks on a company in one sector can affect suppliers, partners and customers in a variety of sectors, disrupting the flow of goods and services on a regional, national or even international scale." In 2003 alone, attacks on cyberspace, via viruses, hacking and identity theft, fraud and industrial espionage have cost the US financial sector nearly $1 billion. The Business Roundtable drafted another report in June 2006 stating that the lack of national policy on Internet reconstitution could undermine the economy and security of the US. Both public and private sectors must commit to focus their efforts and funding on specific capabilities to have strategies and plans in place to reconstitute the Internet following a significant disruption. A coordinated response will help the US and its economy recover more quickly following a cyber attack.

They stress that the development of a private sector and government partnership, focusing on an appropriate response program, will enhance the United States' cyber response position. From the private sector's perspective, individual companies may have adequate plans for their own business interests, but the private sector as a whole is unprepared to work together on a wide-scale. No single critical infrastructure sector owns, operates and uses the Internet. Even in the communications sector, different organizations manage restoration and reconstitution efforts and, in some cases, there are too many organizations without appropriate levels of accountability and responsibility.

Private Sector Reactions to the Russian G8 Initiatives: Preparatory Meetings

The response of private sector firms to the Russian G8 initiative has been very positive. The major Russian companies that have responded favorably so far include: Gazprom, Lukoil,

Aeroflot, Norilsk Nickel, ALROSA and IBS Group. As for international companies, General Electric, SAP, Siemens, Citigroup, Motorola, Microsoft, Telenor and Ericsson have also reacted favorably to the proposal and agreed to cooperate. Finmeccanica has created a public-private advisory board to promote the protected exchange of information between critical energy infrastructure, with one of the factors being the aim of defending against terrorism. WISeKey has established a protected system of communications between governments and businesses in order to effectively exchange information on terrorist threats to cyber-security.

Ericsson has also agreed to cooperate by giving priority-access to public mobile telephone networks for governments (i.e. emergency services in emergency situations). IBS has created a national system of security-information-networks of general use through cooperation between government agencies and businesses, and interaction between national systems. Telenor has established an international network of national Computer Emergency Response Teams through public-private partnerships.

Earlier this year, the Russian Foreign Ministry with the EastWest Institute's support, organized three preparatory meetings with private representatives to gauge their reactions to the Russian and G8 initiatives and prepare for the future. .[3] The discussions focused on three areas: energy infrastructure, cyber security and transport of people, goods, money and services.

Participants at the meetings identified key areas of terrorist threats to:

Energy Infrastructure Security:

1. Direct attacks on energy (hydrocarbon, nuclear, hydro, alternative and other) production and processing facilities.
2. Direct attacks on energy transport and supply routes/infrastructure (pipelines, maritime, electricity grids, etc.).
3. Secondary impact of terrorist attacks on EIS on the public and physical environment.

Cyber Security:

1. Misuse of the Internet for the radicalization of the global population.
2. Use of the Internet by terrorist groups to obtain sensitive information.
3. Threats to communications-based critical infrastructure (Internet and satellite-based).

Transport of People, Goods, Money and Services:

1. Misuse of open or facilitated borders by international terrorists due to a lack of appropriate legal frameworks.
2. Cross-border movement of money to support international terrorist groups and their activities.
3. Cross-border movement of goods as a means for smuggling weapons, nuclear, chemical, biological and other deadly materials by international terrorist networks.

[3] The first preparatory meeting on PPP to counter terrorism was held in Berlin on June 30, 2006, devoted to cross-border movement of people, goods, money and services; and two preparatory meetings took place in Brussels on July 11: on cyber security and protection of critical energy infrastructure.

4. Challenge of balancing the security of the cross-border movement of people, goods and money, and the speed and efficiency of such cross-border movements.

Several recommendations were made at the meetings, some of them touching upon all three sectors:

- First, communications among governments and businesses on terrorist threats can be strengthened. To maximize success, there is a need for closer cooperation in threat-assessment through the active involvement of intelligence and law enforcement agencies in providing relevant information to businesses.

- Secondly, there is a need for stronger interoperability among different local and national security systems. Legislation and procedures governing the cross-border movement of people, goods and money; cyber security and energy infrastructure need to be better coordinated to allow for better cooperation among relevant public agencies and private structures acting in their corresponding roles. Global and sub-regional interoperability needs to be supported by new technologies to increase the security of the cross-border movement of people, goods and money.

- Thirdly, best practices for cooperation between governments and businesses at the national level should be shared in order to institutionalize and internationalize these.

Specific Proposals: October 11 Seminar

Following the preparatory meetings, the October 11th Seminar in Moscow discussed specific proposals submitted by businesses and government agencies on how to improve public-private cooperation to counter terrorism.

Cross-Border Movement of People, Goods and Money

Norilsk Nickel submitted a proposal on how to prevent terrorism financing through precious metals trafficking. *Norilsk Nickel* and *ALROSA*, Russia's largest diamond company, both noted that while advanced technologies and procedures have been enacted at the national level, the lack of harmonized international certification standards and procedures has created a gap that is being exploited by terrorist organizations. Self-regulatory organizations, such as the Kimberly Process in the diamond industry, can play a role in establishing flexible and cost-effective certification procedures, while determining an appropriate trade-off between security and commerce.

Other proposals included: *SAP* on best practices for integrated public-security management; *Citigroup* on a global initiative on remittances as a counter-terrorism measure; and the *Consulting & Marketing International Centre* on the creation of an international insurance fund for terrorist acts and compensating victims of terrorist acts. The *International Center for Consulting and Marketing* and *Rosgosstrakh* underlined the need to go beyond the national anti-terrorism insurance pools created in many countries and to develop an efficient international reinsurance system to protect our societies from major losses resulting from possible large-scale terrorist acts.

Cyber-Security and Communications

Businesses and government agencies presented several initiatives in the field of cyber-security. The *Russian Federal Agency for Information Technologies* submitted a proposal on how to better protect the cross-border circulation of electronic documents; *WISeKey* on the establishment of a protected communications system for governments and businesses in order to effectively exchange information on terrorist threats to cyber-security; and *Telenor* proposed to enhance the role of Computer Emergency Response Teams (CERTs), and to establish an international network of CERTs. *IBS* presented a proposal for the creation of information-networks for general use through the cooperation of government agencies and businesses.

Ericsson put forward a proposal to promote cooperation between governments, civilians and business representatives to establish special telephone networks for emergencies or critical situations. Microsoft recommended that law enforcement bodies upgrade to modern technologies that can better facilitate their work on countering cyber-terrorism, and noted that IT businesses should better support the interoperability of IT systems used by law enforcement agencies. The *Russian Federal Agency for Information Technologies* proposed using universal legal and technological means for creating an international "space of confidence" in the Internet. It would be an effective way to counter cyber-terrorism while simultaneously settling problems, which currently impede business communications development in the fields of electronic trade, telemedicine, distance education, mobile commerce and payments (and a number of other applications requiring legal weight to be given to electronic document circulation).

Critical Energy Infrastructure Protection

Lukoil proposed the conduct of joint exercises between businesses and state agencies to counter terrorism and acts of sabotage. *Lukoil* proposed that the practice of joint exercises between the military and business community should increase in frequency and include more countries. *Gazprom* proposed an enhancement of the role of regional business associations in public-private partnerships to counter terrorism; *Finmeccanica* the creation of a Public-Private Advisory Board to promote a protected exchange of information between energy critical infrastructures.

The *Kurchatov Institute* proposed a new technological solution for the underwater production and transportation of liquefied natural gas (LNG), which would protect tankers from possible terrorist attacks and make them a safer and faster mode of transportation for liquefied gas. *Motorola* presented an action plan demonstrating how information and communications technologies (including CCTV) help monitor critical energy infrastructure and create self-forming networks for responding rapidly in case of emergencies. *EADS* proposed aerospace-based observation platforms as a major contribution in case of emergencies.

Constant and Changing Threats: The Case of Detection Technologies

Throughout 2006, new terrorist plots demonstrated the need for increased and more effective cooperation between businesses and government while highlighting huge unmet security needs. There is no better example of this than the area of detection technologies, one area regarded as being at the sharpest end of partnership between government and the private sector in contemporary counter-terrorism. In August 2006, with little warning, officials in

Britain were faced with the new requirement to detect liquid components for explosive devices in carry-on luggage. Yet the technologies were lacking and the grave disruptions led to sustained criticism by major business interests towards the UK government.

Detection technologies (in particular – explosive detection systems (EDS) and explosive trace detection (ETD) systems) have been in place in airports and seaports for a number of years. Since September 11, 2001, there has been an increased focus on their further development and deployment. The United States – as the primary target for terrorist attacks – has taken the lead in developing and standardizing innovative technologies as well as establishing security norms for other countries. The process of standardization has seen considerable progress. For instance, the same company supplies 93 percent of US Federal Aviation Administration approved explosive scanners used in US airports. However, as the events in August 2006 at Heathrow demonstrated, there is still much to be done to ensure that the right technology is in place to screen and effectively detect potential threats.

Detection technologies are not being applied to a substantial amount of cargo being shipped by air. An estimated 70 percent of air cargo is shipped on passenger airlines and the British Broadcasting Corporation (BBC) reported an industry source stating that as little as half of the air cargo leaving the UK is scanned – and even less in the US. Some argue that it would be impractical to scan all shipments due to their dimensions and time constraints. Conversely, pilot groups are in favor of investing in neutron-scanning technology, which could be used to check all cargo quickly and efficiently.

From the perspective of the private sector – in this context, air- and seaport operators in addition to manufacturers of security products – government standards and legislation provide the benchmark for the development and manufacture of new security products as well as the implementation of security procedures. The private sector also expects governments to put in place an effective decision and policy-making process that will enable the speedy introduction and standardization of the latest technological solutions. Additionally, there is a clear need for an ongoing dialogue between government and business to clarify the needs of the public sector that the new security products are expected to meet, as well as to contribute to the drafting of regulations based on the latest technological development trends.

Conclusion

Over the course of the year's work led by Russia within the framework of the G8, a number of general conclusions emerged on necessary next steps. Participants were invited to:

- Create a synergized anti-terrorist framework and stronger network as the basis for information-sharing and strengthening cooperation between businesses and governments.
- Develop specific legal and political frameworks to address terrorism as a global phenomenon with the active involvement of business and civil society.
- Build on existing national and regional experience to facilitate the transfer of best practices internationally.

- Systematize tasks and delineate responsibilities for businesses and governments so that all parties are equipped to respond to the effects of terrorist attacks.

- Establish a common understanding between businesses and governments on the need for the former to be accorded the status of a leading partner in combating terrorism.

The most general concern that was expressed throughout the meeting was that effective public-private partnerships require:

- Striking the right balance between the imperatives of security on the one hand and, on the other, protecting personal rights and civil liberties

- Building on regional experience and transferring it to the international level

- A law-based approach, accompanied by necessary assistance to countries to strengthen their legal institutions.

All parties must further this initiative. The Moscow Strategy, a declaration of strategic intent to cooperate in this area, launched the process. It will be a centerpiece of the event in November and the foundation for subsequent development. The November meeting is expected to support the continuation of the Russian initiative and its further development in concrete areas through two tracks.

The first track will be an annual international conference with broad G8 and other international representation. Russia will be able to rely on the strong goodwill of its G8 partners to continue leadership in this area should it choose to do so. The international community supports, indeed demands that, this process move forward. There is no need for a new G8 institution but there is a need for continued political mobilization from the highest levels to strengthen public-private partnerships, which has already been demonstrated through the success of the Russian initiative in 2006.

The second track will be the creation of small industry-specific or issue-specific "Working Groups" (such as cyber-security). These groups will proceed at the initiative of the private-sector working with governments to facilitate either the rapid acceptance by governments of emerging technologies from the private sector or more effective communication between governments and businesses from different nations on the mutual need for effective and economically viable responses to terrorist attacks or to the effects of terrorist attacks. The types of Working Groups to emerge in this process will vary from issue to issue, with some governments taking a keener interest in some more than others, and with other Working Groups being of less interest to some governments. Thus, some Working Groups might be led by one or two private companies, with only a small number of governments participating. It would be the responsibility of these independent groups to report to the appropriate intergovernmental groups, such as the G8, APEC or the United Nations.

Given the leadership of Russia and the G8 in this initiative, it is certain that participants in any groups emerging directly from the process will keep in close contact with the relevant Russian agencies and their counterparts in other G8 countries.

Overall there has been a profoundly positive response for the Russian and G8 Initiative from the private sector. Areas of high importance, such as aviation-safety and the financing of terrorist operations, are covered through the Initiative's fostering of partnerships between the public and private sectors. The G8 Initiative fosters a much greater prospect for continuing G8 political leadership and for a variety of forms of concrete cooperation between firms and governments internationally. The G8 Initiative has already led to the creation of new links between companies and foreign governments, and these will surely deliver important contributions to combating terrorism.