EASTWEST INSTITUTE

THIRD ANNUAL WORLDWIDE SECURITY CONFERENCE

Protecting People and Infrastructure: Achievements, Challenges and Future Tasks

Brussels, 21-23 February 2006

IN COOPERATION WITH

MINISTRY OF FOREIGN AFFAIRS
OF THE RUSSIAN FEDERATION

WORLD CUSTOMS ORGANIZATION
ORGANISATION MONDIALE DES DOUANES

TABLE OF CONTENTS

Executive Summary

The Third Annual Worldwide Security Conference identified four major areas requiring further action in the campaign against terrorism that hinder the mounting of a more successful campaign against international terrorism. These are:

- The problem of double standards and different approaches that countries apply in their security policy.

- The political will by the international community must exist to coordinate efforts and set out a clear-cut agenda for action.

- A common definition of what constitutes terrorism is urgently needed to help forge a common policy.

- A balance must be struck between security measures and the personal liberties of our citizens. Lack of progress on this issue hinders the formulation of an effective global strategy.

Partnerships against terrorism require the full cooperation of our societies. The critical challenge is finding ways to engage the private sector, which ahs the means and capital to develop new security technologies while providing crucial on-the-ground information to governments. An effective strategy still does not exist. A strategy must not only set out the general principles for such cooperation, it must also determine priority areas for work to be done. Risk assessment is often not shared among governments or by the private sector. Since it is financially and practically impossible to protect everything, risk assessments should for a major part of our counterterrorism strategy and should be conducted by both sectors in cooperation.

Knowledge and education are as important. Improving awareness is crucial to improving security, whether computer networks, critical infrastructure, borders, trade or public transport. Initiatives to educate the public must therefore form a major part of any counter-terrorism strategy. It is truly a case of being as strong as the weakest link. Meanwhile, the asymmetrical nature of terrorism continues to pose new challenges, forcing us to constantly adapt in order to effectively tackle new threats. A number of new technologies to help us in this effort were detailed during the special technology session. There was widespread agreement that greater emphasis on education and dialogue between the private and public sectors was essential.

Energy security presents increasing challenges, including disputes over resource ownership, depleting resources, and the physical protection of supply lines and infrastructure. To prevent crises, the global community needs to develop a strategy to protect energy infrastructure, to ensure a balance between supply and demand, and to invest in the development of alternative sources of energy, including nuclear power.

Governments need to engage their citizens more seriously in the debate on counter-terrorism.

An informed citizenry can help guide governments towards a balanced risk assessment, which will ensure a proper balance between people's freedoms and counterterrorism measures meant to safeguard those freedoms. Citizens also need to be informed about how to respond in the event of a terrorist attack. Finally, to combat the underlying causes of terrorism, governments and citizens should work together to address and tackle the many factors that form a breeding ground for terrorists. The best way of preventing terrorism is to eliminate the causes that drive people towards terrorism and radicalization as a last resort. We must address poverty and the lack of rights and opportunities at home and abroad - but especially in developing countries. Business can again work side by side with governments in this process, as multinational corporations often have better means to effect beneficial change and possess a better understanding of local realities than policy makers in the public sector.

The majority of participants agreed that it is imperative that we set aside traditional rivalry and distrust, either international or domestic, to combat terrorist threats. International society, individual states, businesses, and the UN must all work together to carry out the social changes that will damage terrorists and shrink the pool of their potential recruits.

Conference participants – by a margin of 80 percent to 10 percent – felt less secure today from the threat of terrorist attack than they did a year ago. There was widespread agreement that the worldwide security processes of the EastWest Institute were helping to break down barriers and create a global cooperative community for dealing with terrorism. Many participants strongly urged that next year's conference achieve even more diversity by including the Middle East in these deliberations. They also urged that the next conference address the effectiveness of efforts to deal with terrorism's root causes, much as this year's conference has successfully brought together the public and private sectors in efforts to strengthen those initiatives that better protect our citizens, infrastructure, and economies.

Welcome and Introduction

John Edwin Mroz, Founder, President and CEO of the EastWest Institute, opened the conference by describing the challenges it faced at its start and illustrated the obstacles to a unified fight against terrorism. He reflected briefly on the origins of the Conference.

There was a need to discuss how to protect citizens, infrastructure and economies (recognized on both sides of the Atlantic). Equally, there was scepticism on both sides as to whether the other was ready – due to jurisdictional and other challenges. Eventually, it was in November 2003 that the first Worldwide Security Conference was held in Brussels, with 150 attendees from both sides of the Atlantic participating.

The issues remain the same throughout all areas of the fight against terror. Lack of trust among nations, suspicion and scepticism has permeated international relations and hinder cooperation and progress.

The potential for progress exists: Since November 2003, the Worldwide Security Conference has grown and the 2006 event featured 400 participants (over three days) from 40 nations, including 80 business representatives, and strong delegations from the Russian Federation, China and the United States. The will to talk and cooperate exists, and there is no reason why governments, the private sector and civil society cannot come together on a more formal level.

Herman de Croo, President of the Belgian House of Representatives, followed Mroz. He explained an initiative in Belgium to fight terrorism that created a new body to facilitate the inter-service flow of information. Belgium is trying to organize all the information the services could obtain in the exercise of their legal assignments. The new body would be controlled by two parliamentary committees, one regarding police, and one regarding intelligence information.

Information sharing is crucial to effectively protecting our societies, especially across borders with international partners. However, domestic agencies must first cooperate and share information with each other before they can be expected to do the same with international counterparts.

Croo spoke of a groundbreaking counter-terrorism act passed in Belgium in December 2005. This act did not limit the definition of terrorism to the planning and committing of assaults, but also included the maintaining of contact with terrorists as a reason for prosecution.

Croo cautioned that when addressing terrorism we must not give in to fear and create laws so stringent that limit our civil liberties. We risk being governed by terrorism, more than governing and combating terrorism ourselves; there is a need to strike a balance between safety and civil liberties.

Michel Danet, Secretary-General of the World Customs Organization (WCO), gave a brief summary of the WCO’s work and importance. It currently consists of 169 members, who manage 90 percent of world trade, and account for 70 percent of world production. Its main goals are the facilitation of trade and providing conventions, recommendations and best practices for the international community. International trade is a factor of development and progress throughout the world.

Following the September 11th, 2001 and subsequent attacks, the WCO, with the private sector and other international organizations, researched securing trade facilitation. The result of this was the Framework of Standards to Secure and Facilitate Global Trade: a document based on the pillars of “customs-to-customs network arrangements” and “customs-to-business partnerships.”

It is a document created by the North and South, balancing two sometimes opposing concepts: facilitation and security. For the North, security is about securing world trade lanes; for the South, security means economic security. The framework thus answers the concerns of all the member countries.

The WCO has started a major program for securing and facilitating capacity-building for customs administrations called "Columbus[1]." The program was launched in June 2005 and will be implemented by nearly 90 customs administrations.

Keynote Speech

Freedom and Security: Getting the Balance Right
Jose Manuel Durao Barroso

Ana Palacio, Former Spanish Foreign Minister and Co-Chair of the EastWest Institute's Board of Directors, introduced the keynote speaker, President of the European Commission Jose Manuel Durao Barroso. She spoke of the issues being debated at the conference as "frontier territory" and extremely complex.

New relationships are needed between the public and private sectors, among social actors, economic actors and policy makers who are politically responsible.

President **Barroso's** speech focused on the challenges to international security, particularly those that concern the European Union (EU). Security has always been the role of governments and it is only through protecting citizens and ensuring their safety that legitimacy is given to power.

The EU is in a unique situation and special problems arise with this special status. Freedom in Europe with no internal borders gives the EU special responsibilities and sadly, criminals were quicker to take advantage of a border-free Europe than law-abiding citizens.

The EU must also address contemporary problems such as international terrorism and all its facets, global pandemics, cyber crime and energy threats. In these areas, it is difficult for individual nations to respond effectively on their own. Global challenges require global solutions.

The Work of the European Commission

The Commission is preparing to work in harness with non-EU member states and also examining ways of creating an effective EU counter-terrorism strategy. Progress has been made by the EU through the creation of EUROJUST, a permanent body of judicial authorities from every member state, and the creation of the European Arrest Warrant.

This measure has facilitated apprehending and extraditing suspects throughout the EU. The warrant helped authorities in the United Kingdom extradite a suspect in last summer's London underground bombings from Italy in just 42 days. Previously, it took an average of more than nine months. The time it takes to bring suspects into custody has taken on increasing importance as the intelligence that might be obtained from them could save many lives.

[1] See http://learning.wcoomd.org/wco_training_capacity_building.htm .

These initiatives also pave the way for greater cooperation with non-EU states. The developments gave the EU a role on the international stage in security affairs, and allowed for the establishment of agreements with third countries over extradition, and legal assistance. Agreements already exist with the US, Norway and Iceland and more would follow.

The Commission's future activities fall broadly into: counter-terrorism and international security; critical infrastructure protection; and assistance and civil protection.

Counter-Terrorism and International Security

The EU is aware of the need for a comprehensive counter-terrorism policy and this proved the catalyst for the adoption of an EU Counter-Terrorism Strategy at the end of last year. The strategy provides a framework and statement of intent to tackle all aspects of terrorism, including radicalization. For the new policy to prove efficient, Member States and EU partners should cooperate more closely, and customs provides a good example of this.

Increased border controls should lead to greater cooperation among the member states and their partners, thereby allowing them to more effectively address other issues such as money laundering and other illegal financial-related activities.

Cooperation among states is not enough to win the war on terror. The scale and nature of the threat requires partnerships between governments and the private sector. These partnerships assume increasing importance considering that a significant percent of our national infrastructure is owned and operated by businesses.

Critical Infrastructure Protection

EASTWEST INSTITUTE
THIRD ANNUAL WOR DE SECURITY CONFERENC
rotecting People and Infrastruc hievements, Challenges and Future Ta
2006

Our augmented dependence on critical infrastructure would cause us to feel the consequences of a terrorist attack immediately. Our increasing cooperation has in some ways rendered us more vulnerable since much of our infrastructure is now inter-connected, damage to an installation in one state can have a 'domino' effect on its neighbors.We cannot realistically hope to safeguard all aspects of critical infrastructure. We can secure major installations but massive networks such as pipelines are impossible to fully protect. The challenge is to minimize risk, while protecting privacy and our quality of life in a cost-effective way. Energy and transport sectors are of particular importance - without energy, our societies would virtually grind to a halt.

Crucial to safeguarding all infrastructure is the protection of critical information infrastructure. Technology is now embedded in our modern lives and almost everything is dependent on computer-operated systems – from telephone exchanges to traffic light systems to nuclear power stations. Essential infrastructures, such as power grids, water systems and telecommunications, depend on information networks that span the globe. Cyber security is thus also essential to the daily well-being of our citizens.

These factors have changed the nature of security irrevocably and we must adapt to it. The era of more open borders, integrated economies and new technologies has thrown up new security challenges. Military threats posed by hostile states have been supplemented by new, dynamic threats that can disrupt our society and endanger our citizens.

Assistance and Civil Protection

The last pillar of activities concerns assistance and civil protection. When prevention fails and attacks occur, only a carefully organized and effective response system can mitigate the consequences and guarantee a quick return to normality.

Two years ago, the member states of the EU pledged to use all the instruments at their disposal to assist any member state affected by terrorist attacks. The Commission is also ready to assist through the Community Civil Protection Mechanism. Any country struck by a major disaster can call upon the mechanism, and this includes terrorism.

Whenever a disaster strikes, it alerts a network of national civil protection authorities. The country in need can then request assistance, and the mechanism will send coordination experts to ensure the smooth distribution of assistance. During 2005, it provided assistance to Portugal to help deal with forest fires, and the United States (US) in the aftermath of Hurricane Katrina.

The Commission recently presented a legislative proposal to develop these activities and ensure that the EU is in a position to respond positively and decisively to any request for assistance. Political support and funding are essential to translate this ambition into reality.

Barroso ended with a statement of intent and hope: “Working together, we can get the balance right for our citizens: not freedom or security, but freedom and security.”

Session One

Double Standards and Multiple Approaches: How to Overcome Political Obstacles to a Truly Global Response to International Terrorism?

George F. Russell, Jr. Chairman Emeritus of Russell Investment Group and Russell 20-20 and Co-Chairman, EastWest Institute’s Board of Directors, introduced the first session of the conference by urging both speakers and participants to meet the challenge of the conference of determining a common response to international terrorism.

This first session began with a presentation by Ambassador **C. Boyden Gray**, the US Ambassador to the European Union, who stressed the importance of international cooperation in the fight against terrorism and called for greater cooperation between the US and the EU.

Gray illustrated the progress made since 9/11 by relating some of the steps taken by the US and the EU – specifically in the area of law-enforcement and judicial cooperation – towards fostering closer and more productive relations.

Agreements reached included those on extradition and mutual legal assistance. The Ambassador was clear also about the vital importance of working with the United Nations.

This fostering of relationships is a continuing process. Much is being done to establish, broaden and deepen working relationships with EU institutions. Agreements with EUROPOL have already been reached and agreements with EUROJUST are underway.

.
Gray drew attention to Euro-American collaborative efforts in homeland security and border control, namely the sharing of passenger name records and agreement on the use of biometric technology in travel documents. Another joint initiative has been INTERPOL’s creation of a database containing information on lost and stolen passports. The U.S. and EU are also advocating stronger security cooperation through the World Customs Organization and other international organizations.

Ambassador **Anatoly Safonov**, Special Representative of the President of the Russian Federation for International Cooperation in the Fight Against Terrorism and Transnational Organized Crime, who drew attention to the third day of the conference and the Russian initiative to strengthen partnerships between the public and private sector in counter-terrorism.

Russia believes that the fight against terrorists should be in strict compliance with international law. The central role of the UN in international counterterrorist cooperation is indisputable for Russia. International law and the UN provide the most effective framework and legitimacy for the international fight against terrorism. This requires the introduction of new laws in many states and they will be more inclined to accept these changes if the international “powers” are seen to be acting in accordance with international law.

Radicalization is a major concern, on par with terrorist financing.

The world is working in harness towards improved relations and mechanisms for tackling terrorism.

Work has begun on a comprehensive UN counter-terrorism strategy, which will provide a much needed reference point and the birth of an international norm to which all states must subscribe. Variation in legal, political and financial standards creates new possibilities for terrorists.

Russia wishes to broaden cooperation against terror to include the world of business and society as a whole.

Gijs de Vries, Counter-Terrorism Coordinator for the European Union, spoke next and illustrated cooperation among member states with the example of a terrorist suspect successfully prosecuted as a result of cooperation among EUROPOL and the Irish, Dutch and French police forces.

Terrorism is a global problem with local ramifications that must be addressed locally, regionally, and globally. The challenge in the EU is to incorporate both the domestic and foreign policies of the Member States to create a singular policy for the EU. In the EU, national forces are not inefficient. What is needed is improved cooperation across borders to make these national processes as effective as possible. The European arrest warrant is a perfect example of the progress that has already been made in this process.

The EU has been active regarding standards, particularly at European airports, and the Commission has made recommendations to member states. The aim is to respect national sovereignty, while ensuring that no country is the weakest link in the chain. One of the key roles of the EU is assisting the operational work of the member states' national forces. Bodies with this aim are EUROPOL, EUROJUST, FRONTEX and the Brussels-based Situation Centre. In these bodies, the model is one of information exchange, the establishment of best practices, and cooperation - the aim being to assist the decentralized national forces in doing their job more effectively.

More "hands-on" initiatives are underway including networking the special intervention units in Europe's police forces. Customs services have organized the first multinational exercise in monitoring borders. Six exercises on emergency management coordination will take place in 2006 with the member states working together across borders.

At a global level, the EU is intent on strengthening the role of the UN. The Union is aware of the need to assist developing states in implementing new conventions and legislation.

The EU is also working with other international bodies, including the International Atomic Energy Agency and the OPCW, to address weapons of mass destruction. The EU is also working with Russia and the Ukraine on other issues.

Work is underway to address the roots of terrorism by taking action in a number of countries in the Near and Middle East and, under Austria's presidency, the Balkan region has become a specific priority. It was also working to address the issue of poverty, often believed to contribute to a climate in which radicalization becomes more likely.

The war on terrorism is a global battle in which all must cooperate on the basis of an allegiance to the UN Convention on human rights and the Universal Declaration. These should prove universally binding across religious, ethic and national boundaries.

Gao Jian, Director General of Security for People's Republic of China's Foreign Ministry, also argued that the global threat of terrorism requires a cohesive global response and then identified the obstacles to international cooperation. Definition is the biggest problem, as discrepancies affect all aspects of cooperation against terrorism – from defining terrorism itself, to defining what constitutes a terrorist to defining best practices and methods for tackling the problem.

Religions and countries should not be labelled as "terrorists" or terrorist "sympathizers." This does not help to win support or isolate terrorists. All ethnic groups and major religions in the world believe in and long for peace.

Multilateral action is of paramount importance. Rather than acting unilaterally, the international community should take the time to press for a peaceful solution through dialogue, communication and international mediation. We should try to adopt a more preventive approach to terrorism.

For successful cooperation against terrorism, it is imperative to respect international norms, in particular national sovereignty and the concerns of other states. China fully supports the leading role played by the UN in anti-terrorism and calls for the early formulation of a comprehensive convention on international terrorism, which can serve as a legal basis for cooperation. The UN is the only body that can objectively lead all states, irrespective of ideologies and governments, in the fight against terrorism.

The developed nations of the world must do more to address poverty. Providing evidence of the compassionate and benevolent nature of the international community would strike an important blow for example in the ideological battle being fought by the extremist Muslims and would diminish their opportunities for recruitment.

Dialogue among nations is vital and China desires to work closely with other nations towards a lasting peace and common prosperity.

Boris Mylnikov, Head of the Anti-Terrorist Center of the Commonwealth of Independent States, stated that formally there are no barriers for international cooperation between states but in practice each government responds to terrorism according to its own national interest.

The legal system in a country, though supposed to address the needs and circumstances of society is always reactive, having to adjust to the situation every time. Thus there are insufficient measures to protect against terrorism. Legislation is lacking in the national and international framework.

At the international level there are double standards when evaluating what constitutes a terrorist threat. It is necessary and a priority to tackle the underlying causes but in order to tackle the threats caused by terrorists, one must first agree on the definitions of the different terms.

The Anti-Terrorist Center of the Commonwealth of Independent States (CIS) has developed an approved vocabulary consisting of definitions of terms of terrorism and extremism. Similar work should perhaps be undertaken at the international level.

Germany went through periods of terrorism during the 1970s, and used an approach of strict measures against the terrorists while simultaneously trying to tackle the underlying causes. These included preventive measures with regard to radically-minded persons who had not yet committed terrorist acts.

This German approach might be useful in the development of further international legislation on counter-terrorism.

The principles to guide counter-terrorism measures must include political, economic, social, legal, educative, as well as investigative or even military measures. This wide spectrum of measures would guarantee a proper balance between security and human rights.

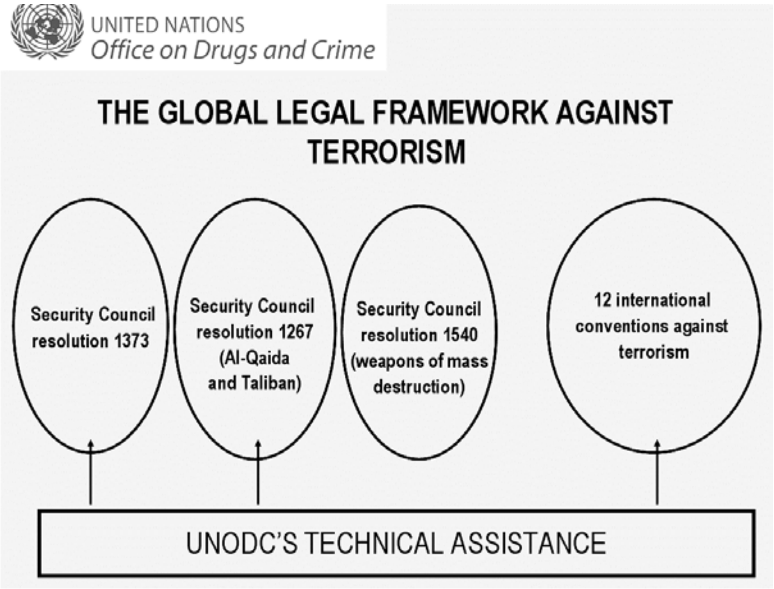
Session Two

A Common Public and Private Area of Concern: Financial/Critical Economic Infrastructure and Security

Maria L. Cattaui, former Secretary General of the International Chamber of Commerce, opened the session, noting that in addition to the issue of terrorist financing, the financial infrastructures have become primary targets for criminals, terrorists and other "troublemakers."

Walter Gehr, Project Coordinator for the Terrorism Prevention Branch of United Nations' Office on Drugs and Crime's, argued that a wide range of important financial issues regarding security and international cooperation are "grey areas."

States must be convinced to subscribe to and impose international laws dealing with terrorist financing such as the International Convention for the Suppression of the Financing of Terrorism. Although 149 states are bound by the convention, double standards continue to exist in the international community.


UNITED NATIONS
Office on Drugs and Crime
THE GLOBAL LEGAL FRAMEWORK AGAINST TERRORISM
Security Council resolution 1373
Security Council resolution 1267 (Al-Qaida and Taliban)
Security Council resolution 1540 (weapons of mass destruction)
12 international conventions against terrorism
UNODC'S TECHNICAL ASSISTANCE

To freeze the assets of terrorists, the issues are: What terrorist funds? Who is a terrorist? This problem should be resolved by the fact that the UN Security Council has issued a legally-binding list of members, persons and entities associated to Al-Qaeda and the Taliban. The assets of these persons have to be frozen instantly.

Until any new convention on terrorism is introduced, we must work with the tools currently available to us.

Al-Qaeda is obviously not the only terrorist organization; there are other terrorists who fall under UNSC Resolution 1373 and the Convention on the Suppression of Terrorist Financing and they pose an equal challenge to financial regulation and systems.

Perhaps the biggest issue is monitoring financial flows – unusual, complex and big financial transactions. Software has been developed to detect unusual and suspicious transactions but development in so many different countries immediately poses questions of standardization and compatibility. It is unknown whether these software programs are even compatible with the UN sanctions regime.

The private sector is at the forefront of profiling customers and Interpol has developed a study to profile those who are likely to finance terrorists. There are, therefore, a vast number of actors that must work closely together. These include financial institutions, both public and private within these states and also international organizations such as Interpol. The UN must provide the relevant standards and criteria for international society in order to ensure compatibility.

The Organization for Economic Cooperation & Development's (OECD) Financial Action Task Force (FATF) has a prominent role because it gathers representatives of the ministries of finance. It does not however gather all relevant parties and some confusion is therefore likely to ensue as a result of lack of communication. The FATF's 40 recommendations for countering money-laundering and nine special recommendations for countering terrorist financing are, however, the international standards endorsed by the UN.

The initiatives and purpose of other financial groups fall into grey areas. The UN is unsure of the role and impact of the Egmont Group in the work of bankers and also the role of the international organization of the Security Commission.

The biggest challenge posed is the fact that all of the responsibilities in combating terrorist financing are shared tasks involving multiple parties.

Fabio Marini, Head of Unit for the Fight Against Economic, Financial and Cyber Crime of the European Commission spoke on recent European developments in financial and economic security.

The Commission is proposing new legislation; proposing best practice; and developing specific policies for the protection of financial and critical economic infrastructure. The greatest concern of the financial sector is the threat of economic disruption by terrorism. This risk is enhanced by the computer interconnectivity used by the financial services. A successful attack would be disastrous. The financial markets and other forms of infrastructure - telecommunications, the energy industry, and the Internet – characterize the vulnerability.

We need clear, well-identified goals for the protection of critical infrastructure against attack or disruption, supported by a centrally coordinated campaign. These goals should include defining the roles of relevant actors to ensure that we have the necessary resources to assess vulnerabilities daily.

The Commission is also working to close down terrorists' financial resources in accordance with the FATF's recommendations, a recent example of this being the Third Money Laundering Directive, adopted in September 2005.

It is simple to detect transactions involving large sums of money. However, the London bombings cost just €1,000 – a small sum and one that would not trigger any alarms. Another problem is that the transfer may begin legitimately and become illegitimate later – further complicating the detection process.

Aldwin Wight, Vice President for Strategic Development at Kroll Security Group, spoke next. Wight was also able to offer an important and different perspective to the subject as an operator, having served extensively with Britain's SAS. He argued that the principles for effective counter-terrorism, no matter the area, are readily apparent: cooperation and coordination, adding that sometimes, we miss central direction.

Terrorists are entrepreneurs who seize opportunities to raise capital, among them: raiding banks, getting inside banks, scams on euro subsidies, drugs, acting as consultants for other terrorist groups, protection rackets, etc. The Internet also provides a major source of funding from online scams and to deal with counterfeit goods.

Chris Painter, Chair of the Hi-Tech Crime Subgroup of the Group of Eight, closed the session, giving an overview of the initiatives being undertaken to safeguard the critical information infrastructure that is vital to today's financial markets.

Both financial and information infrastructures are cross-border, international and interconnected. As a result they also present a number of vulnerabilities. Since our financial and power sectors, societies and governments have become more dependent on information infrastructure to communicate and transact business, the effect of a criminal attack on this is amplified and affects multiple sectors.

A few years ago, a special meeting of the G8 brought together those persons involved with protecting critical infrastructure and also responding to any threats and attacks. The result was a document detailing what was needed to effectively achieve this. Effective protection requires communication, coordination and cooperation, nationally and internationally, among all stakeholders – industry, academia, the private sector and government entities, including infrastructure protection authorities and law enforcement.

Governments can provide the legal framework to criminalize certain acts, enforce laws and adhere to additional policies on the issue. This framework must be developed in consultation with the private sector.

Session Three

Security and the Role of Technology

The final session of the first day of the Conference focused on the issues identified during the previous year's conference and subsequently examined by the EastWest Institute's Consortium on Security and Technology. Dr. **Vasil Hudak**, Vice President and Director of the EastWest Institute's Brussels Center, chaired the session and began by explaining project.

One of the outcomes and strong messages of the Second Worldwide Security Conference was the call for better cooperation and dialogue between public and private sectors. EWI's response to this was to establish the Consortium on Security and Technology.

The group currently consists EWI and eight corporations: Microsoft, SAP, General Electric, Accenture, AIG, Sun Microsystems, CapGemini and Canberra, in addition to officials from the EU and member states. It meets on four key cluster areas: cyber security, critical infrastructure protection, customs and border control and biometrics.

The meetings are limited, closed and confidential with Chatham House rules applying. This allows for real interaction of the private and public sectors on the issues at the intersection between security and technology.

Scott Boylan, spoke next on the topic of critical infrastructure protection.

He first posed the question: What do we need to secure those types of facilities? He then explained that there are the elements of cost, reasonableness and intelligence on what exactly the threat is.

Technology can provide intelligence on the terrorists to both governments and businesses thereby assisting in dedicating resources, and making decisions as to how to protect infrastructure. Technology can be used to identify terrorists from simple surveillance to its use in data analysis to uncover trends and information. Intelligence is important as terrorists can be one's employees, the people that have access to this key infrastructure, and that has to be part of the consideration.

The four key areas with the potential to cause major damage are: air transit, mass transit, nuclear facilities and chemical sites. This is recognized by the relevant authorities but they need to act faster.

Governments must act quickly and prudently on the security issues that require attention. Government standards and legislation are integral to the security contribution of the private sector as they provide the benchmark for development, production and general security.

Technological Trends

Communication is an area of crucial importance in all security fields and technology is no exception. Communication between the different technologies must improve. There are many technologies that do not talk to each other.

Trace applications are able to identify traces of a substance on a person or object and technology continues to improve. It is now being adapted and incorporated into different security appliances, such as ticket machines for mass transit.

Companies in the security area are working to increase the explosive detection capabilities at checkpoints. Trace applications can also be used to test for drugs, helping ensure safety and efficiency.

Sean O'Brien, Industry Director for Public Security (EMEA) for SAP, spoke next.

We must be aware, when discussing security, of the difference in resources of the individual countries involved. However, in spite of the need to recognize the fact that countries have decidedly different situations and budgets, we must also recognize that our security is interlinked.

The debate on public security is very active. We need thought leadership on where it is going. It is a sector in which there is a lack of innovation, competition and risk mitigation, meaning there is a greater focus on transforming existing measures and facilities. Cost is important, in particular how we can get more for less. We must examine and learn from other industries.

What is needed in public security involves numerous factors including identity management with passports, visas and identity cards with biometrics. Regarding the way governments operate in the area of identity, there are intelligence systems, police systems, court systems, and border control. Often, these do not communicate.

Public security comprises counter-terrorism. Since 9/11 this has been of increasing importance along with the facets it encompasses – intelligence gathering, interoperability, intelligence sharing, etc. In the last few years we have been reminded that preparedness for emergency crisis management is something that is necessary not just for terrorist situations but also for non-man-made threats such as avian flu, storms, floods and tsunamis. Security requires far more than addressing simply manmade deliberate threats and attacks.

Critical infrastructure is everywhere and we cannot hope to safeguard it all. It is a question of performing risk assessments and then implementing security countermeasures. Agencies must work together and this is another reason why we need common understanding.

With common understanding an overarching framework for an integrated public security strategy is possible. This would allow a roadmap for transformation and clarify the issues for the private sector.

The challenges faced by public security organizations are often the same as those being faced elsewhere. SAP works with the Koordinierter Sanitaetsdienst (KSD) in Switzerland. Their collaborative work focuses on disaster and crisis management, including a solution that enables the fire, medical, military and police services to coordinate their response.

Development of best practices is also important. Security is not just about technology – it is also about changing the way people operate and enabling organizations to work differently. Both the public and private sector need to play a role in making the security market more open, since without innovation the problems of the past will be repeated.

If there is no big picture and roadmap, technology companies won't have clarity about the direction things are moving in, and therefore cannot align their solution strategy to those different changes.

Biometrics was the next topic discussed, as **Max Snijder**, CEO of the European Biometric Forum presented.

There is a gap between biometrics as a technology and the perceived high-level possibilities which biometrics provide. Biometrics can be an extremely useful tool to enhance security, but it is not a "be all and end-all" solution.

Biometrics is an extremely strong and unparalleled means for identification. It can increase security, convenience and efficiency so long as it is dealt with correctly.

The most obvious area for the integration of biometric technology is border management. In this sector there are a wide range of applications.

To ensure that biometrics are up to the task, manufacturers need to be provided with guidelines as to what governments require and targeted scenarios for the use of the technology.

Each scenario should describe the different roles of biometrics. Biometrics can be only one part of a solution, one link in a long chain. The impact of biometrics on our security depends on the role we expect it to play, the application, design and the underlying legal framework.

A major challenge is obtaining consensus on how exactly biometrics, and relevant personal data will be handled. Privacy, data protection, security and trust are the key issues and they require common frameworks. Without agreement on data privacy and management the international community will not achieve a harmonized and effective use of biometrics in passports.

The final challenge to biometrics is the human element. Technology works when handled properly. If operators are insufficiently trained, technology can destroy an entire system. It is through human vigilance that biometrics can prove to be effective.

The biometrics element should be integrated into all discussions on border security and its cost-benefit risk must be assessed, both in financial terms and in terms of efficiency. It is necessary to determine which risks are being mitigated and whether current actions have introduced new risks. Also, common definitions on application profiles must be created.

The final speaker in the technology session was **Stephen McGibbon**, Senior Director of Microsoft's EMEA Technology Office and Chief Technology Officer for Eastern Europe, who addressed recent and future developments in cyber-security, electronic identity and biometrics.

The nature of cyber-security has changed completely. The threat model for personal computing changed has. Customers have upgraded to broadband and now leave their computers on all day. The machines were not designed for this kind of usage. They were designed with a particular threat model in place but are now being used in a totally different environment.

Microsoft had to respond to this change, as it became apparent that the design points for Windows 95 and some of the earlier versions of Windows XP were extremely vulnerable to this threat environment. The first initiative was called the “trustworthy computing initiative” and focused not just on security but also on privacy, reliability and availability as the other attributes of a trustworthy system.

The behavior of hackers has also changed. In the past, if a computer obtained a virus or was being hacked, one was made aware of the attack. Now hackers are more motivated to disguise their attacks so that they are able to conduct illegal activities through one’s computer.

Microsoft now works with law enforcement agencies to communicate and address threats. This involves providing them with access to technical information and assisting their specialist departments with forensic work. This support is provided to the prosecution stage.

Electronic Identification (E-ID) is an interesting area, although highly complicated. ID cards themselves are a simple concept. Electronic ID (E-ID) cards, however, pose a variety of different problems relating to the legal frameworks around them.

In the EU this issue is further complicated by what each country believes should be recorded, the legislative framework for the cards and what they should actually be used for. It is likely that there will not be a single European identification law that will support community-wide cards. Instead, there will be a series of identity cards issued by the individual member states reflecting their national legislation. National E-ID cards also present the challenge of devising a way to inter-operate them and make them compatible with each other. The question of compatibility is not a technological issue but one of reaching legal agreement between states.

Adding the issue of biometrics makes it even more difficult to reach agreement on identity cards. We should be wary of the potential for abuse of biometrics and personal data. The technology can be implemented for one purpose but then misused to infringe on an individual’s privacy.

Session Four

Getting the Balance Right: Preventing Terrorism, While Protecting our Societies and Preserving our Freedoms

Kim Campbell, Secretary-General of the Club of Madrid and former Prime Minister of Canada, chaired this session and drew attention to both the complexities of and obstacles to implementing effective, non-intrusive legislation, and the importance of obtaining a balance.

Matthias Sonn, Director of Germany's Task Force on International Cooperation in Combating Terrorism, opened the presentations and immediately focused on the need for cooperation in the fight against terrorism.

Security policy is a problem that can be tackled effectively only if Europe and the US work together with a common purpose. Because modern terrorism is a global threat, national and regional combative efforts are not sufficient. Trans-Atlantic partners must join forces and act together so that security, peace and prosperity are guaranteed.

Europe and North America must come together to fight terrorism for the same reason that they have become the targets for global terrorism – they are committed to the same fundamental values of freedom and democracy, the values of Enlightenment and democratic secularism. The target for the terrorists is the open society that we jointly stand for.

Combating the threat of international terrorism must encompass action over a wide range of areas: in the economic and political sector, in intelligence and police work, and, where necessary, in the military domain. Prevention is the most important factor in fighting terrorism. UN Secretary General Kofi Annan has observed that it is more effective to prevent people from becoming terrorists than to prevent terrorist acts.

Prevention raises a number of challenges. It requires intelligence work and data, and also cutting off the supply of potential terrorists to effectively eliminate terrorism (this is a hugely complex task). We need to ask ourselves many questions – Why are more Muslims in Europe becoming radicals? Is there a link between the integration (or lack of) of Muslims and their increasing radicalization / recruitment as terrorists? What can Europe and the US learn from each other's efforts to prevent radical ideas from gaining ground or to curb the recruitment activities of terrorist groups and organizations? Why is it that some of the best-educated people tend to be some of the most radical ones? What answers do these individuals find in radical organizations that our free societies are apparently not giving them?

Exploring and understanding these factors will help us not only employ military and police instruments effectively, but also successfully address the political and social conflicts which contribute to the underlying factors that can lead to terrorism. It is overly simplistic to say that poverty leads to terrorism but it is safe to assume that political and social conflicts (in a larger sense) contribute to the problem.

Were we to trade many of our liberties for greater security, this would result in the greatest victory for those hoping to attack our values.

Islam is not the enemy and it should not be equated with Islamist-inspired terrorism. Any confrontation between the secular democratic world and Islam would be a victory for the terrorists and a defeat for all humanity.

Europol's **Peter Gridling**, Director of Europols's Counter-Terrorism Unit spoke next.

We should be careful of exaggerated and detrimental media coverage. Reporting and speculation on bigger and more spectacular future attacks, or the use of biological and chemical agents, nuclear materials or strong radiological sources does not help to reassure the public of its safety and security. Fear does not mean threat, and perception is not reality.

Europol delivers valuable assessments, tailored operational support and centralized reference tools to member states and other partners. Its counter terrorism response is organized around two programs – a counter-terrorism program which combines all counter-terrorism mandated areas and a counter-proliferation program that deals more with the new threats of CBRN means.

The organization has priority activities: monitoring trends and developments in terrorism; providing operational support to member states and their investigations; carrying out strategic and operational analysis in the field of terrorism; assessing threats and the risks; and raising awareness of the relevant issues among law enforcement personnel, representatives of other authorities and political decision-makers.

Europol has also developed a preparedness program, which provides not only facilities and resources, but also a 24/7 crisis response. Complementary to this, counter-terrorism awareness training is provided by Europol when requested by Member States.

The primary objective for European counter-terrorism strategy must be the protection and the maintenance of our liberal democracy and the strict application of rule of law in the fight against terrorism. This is something that Europol is determined to ensure.

Frank Urbancic, Principal Deputy Coordinator for the US Department of State, began his presentation stating that security and civil liberties are not and cannot be allowed to become mutually exclusive.

Civil liberties cannot exist unless our societies are protected from those that seek to harm them. We also, however, cannot allow fear of terrorism to lead us to excessively curtail our liberties and so inflict lasting harm on the values that we are struggling to defend. A balance can and should be created that does not infringe too much upon freedoms, cross-border trade and travel.

These issues require careful consideration and evaluation. As the nature and level of the threat varies so must our response. The manner and level of our response should be exponential to the threat. This is complicated by the fact that terrorism does not follow conventional means or conduct war in the traditional sense.

Terrorists deliberately attack civilians to disrupt or destroy the liberal democratic world. Terrorists are capable of adapting quickly to new circumstances and environments. Intelligence has shown that they are often well educated and aware of how to exploit our free societies. The media and the Internet, the speed and minimal expense of travel and communication, provide examples of this practical know-how and how recent advances have made possible the easy and trans-national movement of operatives, expertise, money, and explosives.

We must cut the links between al-Qaeda and its affiliates – finances, intelligence, communication, cultural affiliation, training, and other support infrastructure. To achieve this, a counter-terrorism strategy must simultaneously attack terrorist "safe-havens" and the underlying conditions that terrorists exploit to advance their cause. "Safe-havens" should include geographic, cyber and ideological spaces. Another target is socio-political factors that might be exploited by terrorist organizations.

Such a strategy requires the use of all tools of statecraft and its scope is such that it requires in-depth international cooperation to be successful.

International cooperation is vital to the successful closing of terrorist "safe-havens" as most of these exist astride national borders or in ungoverned areas. The Pankisi Gorge in northern Georgia provides an example of international cooperation and success in clamping down on terrorist safe havens.

In 2002, the US, as part of its ongoing efforts against al-Qaeda, made an offer to the Georgian government to train and equip several battalions of the Georgian army to reassert control over hundreds of heavily armed and battle-hardened fighters in the Pankisi Gorge.

With the support and assistance of the US, the Georgian government succeeded in not only driving the terrorists out of Pankisi Gorge, but also in preventing their return.

Our most important task in the war on terror is not the "destructive" one of eradicating enemy networks, but the "constructive" task of building legitimacy, good governance, trust and rule of law.

The fight against terrorism might take decades. We must remain conscious of what we are fighting for and ensure that the actions we take and the policies we pursue do no harm our liberties. US, he said, is convinced that these two objectives are both consistent and mutually reinforcing.

The penultimate speaker was **Rutsel Silvestre J. Martha**, Interpol's General Counsel, who stated that it is not necessary to assume that preventing terrorism and observing human rights and fundamental freedoms are opposing counterparts that require reconciliation.

For those who work in law enforcement the adherence to human rights and freedoms has become integral since there have been many instances in which either an investigation or cooperation, simply collapsed or was denied due to the non-observance of fundamental rights and freedoms. If Interpol did not have a system in place that guaranteed these fundamental rights and freedoms, it would no longer exist.

Interpol's key role is to facilitate cross-border police cooperation and to support and assist all organizations, authorities and services whose mission is to prevent and combat terrorism. The organization does this by providing secure and global police communication services.

The agency also provides operational data services and databases to police forces, which allows them to directly access information that may aid their crime investigations or preventive work.

Interpol maintains a range of global databases covering key data including names, individuals, wanted persons, fingerprints, photographs, DNA, stolen and lost identification documents and travel documents to assist police forces. Interpol also provides operational police support services addressing fugitives, terrorism, drugs and organized crime, human trafficking, financial and high-tech crime, the sexual exploitation of children on the Internet, stolen vehicles and bio-terrorism. Interpol also alerts police to wanted persons via graded notices.

There have been calls to stop the flow of criminal information through Interpol and to eliminate data from its files. These sources of information and Interpol have survived because the protection of fundamental rights and freedoms are at the core of the organization's system.

Interpol's constitution demands the observance of the spirit of the Universal Declaration of Human Rights and also prohibits any intervention or activity that is political, military, religious or racial in character. As a result, countries can cooperate through Interpol without fear of being in breach of the law. Members of Interpol are increasingly citing the observance of human rights as a prerequisite for their cooperation, a fact which makes it even more critical for Interpol to ensure that its global databases and the exchange of information conducted via its channels are not tainted with doubts concerning the observance of fundamental rights and freedoms.

The final panelist, **Jamie Shea**, Director of Policy Planning at the Private Office of the Secretary General of NATO, detailed NATO's actions towards protecting citizens.

Terrorism is an extremely effective means of gaining attention and pushing a political agenda – at least in the eyes of the terrorists. Shea pointed out Bin Laden's oft-vocalized pride in the fact that for every dollar terrorists spend, we potentially spend billions of dollars to protect ourselves. This is proof that the cost-benefit ratio is clearly on their side.

In addition to the economic advantage, he explained that there is no shortage of recruits for terrorist organizations. This ready supply of recruits can be attributed to the many unresolved conflicts around the world and the anger that fuel international terrorists.

Two interlinked questions must be asked: Are we doing enough and are we cooperating enough? In addition, another issue to be resolved is moral clarification. A significant percentage of people worldwide believe that terrorism is a form of freedom-fighting and that attacks on civilians are justified. This can be attributed to our failure to provide a common definition and analysis of terrorism.

Moral confusion goes both ways. Another question is whether freedom of speech is absolute even when it is certain to be inflammatory and cause moral outrage. In the Middle East, people have been pointing out that in Europe we justify cartoons lampooning Islam but we imprison a British historian in Austria for denying the Holocaust.

What is badly needed internationally is a moral framework so that we know what we are dealing with in terms of how we describe religion, how we define terrorism, violence and the response to acts of violence. International organizations should be brought together under the United Nations to define a common, mutually-accepted plan.

A question and answer session followed.

Independent Advisor and Law Enforcement and Security Consultant, **Nicholas van Helten** asked how much was actually being done by intelligence and law-enforcement agencies to cooperate and work together.

Peter Gridling, Director of the Counter-Terrorism Unit at Europol, answered, saying that it is his belief that Europe needs an attack on the scale of 9/11 to understand the meaning of cooperation and overall responsibility and that the intelligence community is particularly reticent about collaborating with partners.

Shea strongly disagreed with Gridling's statement, calling it "perverse," and pointed to the many successes of the European intelligence services in preventing terrorist attacks.

Another provocative topic was **Ricardo de Rituerto**, Correspondent for *El Pais*, who questioned the balance between civil liberties and the fight against terrorism when looking at current US foreign policy.

Urbancic believed there are no contradictions in US rhetoric and US actions when it comes to civil liberties and the fight against terrorism.

There, is, however a new situation to deal with, for which the US is seeking approaches. This new situation is a new world, not one that fits into the American Constitution written in 1789 but a world that we all have to deal with.

Break-Out Sessions

Customs and Border Control

Cattaui opened this session, which focused on the capacity of international organizations and countries to respond to crises and protect the public in an emergency.

NATO's Director of Civil Emergency Planning, **Carsten Fausbøll** took the floor and spoke about the functions of NATO's Euro-Atlantic Disaster Response and Coordination Center.

The Center has developed the capacity to respond to chemical, biological, bacteriological and radiological emergencies. It regularly organizes exercises to prepare for such disasters, including those caused by weapons of mass destruction.

Ian Abbott, Chief of the Policy and Planning Division of the EU Military Staff, began by stating the "five facts of life" on civil protection and coordination:

- Democracies are usually *reactive* and not *proactive*.
- The sharing of intelligence is probably a misnomer. It should be described as the trading of intelligence.
- Existing organizational structures encourage duplication with the underlying principle that such duplication is not always effective – and that means that they are more "silo-driven" than "lateral."
- We are failing to coordinate our collective efforts.
- We are failing to communicate to the public.

Cattaui said that the message arising from the discussion is that we need to involve the private sector comprehensively rather than merely relegating businesses to a consultant's role.

Businesses must also be involved at a local level, where they have already built trust with local authorities and where there is a proven track record of cooperation on an operational level.

Ultimately, there is a need for true partnerships in the field of civil protection and crisis response. Partnerships should not be commercial arrangements. Shared responsibility and greater collaboration is imperative.

Cyber Security

Ronald de Bruin, Head of the European Network and Information Security Agency's (ENISA) Cooperation and Support Department, began with an overview of the cyber security paradigms:

Critical Information Infrastructure Protection (CIIP), Cyber Crime and Network and Information Security. The forces driving these paradigms are the differences between them. CIIP is driven by the National Security and Defence establishment, Cyber Crime by the Law-Enforcement Community and Network and Information Security by Information Society and the Digital Economy. The common ground is the interest in Awareness Raising and Promotion of Best Practices. Today's society and economy depend heavily on networks and information systems. This has created the need for a culture of network and information security.

With this in mind, he stated that ENISA sees its tasks as the following:

- Risk assessment and management
- Track standardization
- Information exchange and cooperation
- Promoting Computer Emergency Response Team (CERT) cooperation
- Promoting best practices
- Raising awareness

ENISA's goal is to become a resource and expertise center for the European Commission and EU member states, and to facilitate communications on cyber security both within the EU and with outside actors.

Painter presented his vision of the role of law-enforcement in cyber security and the technical challenges that law-enforcement agencies are facing in this field – for example, the criminals could be thousands of miles away from the company they are attacking and they could re-route to cover up their trail. Another problem is that companies do not have to report cyber attacks against them and, due to concern for their reputation, often do not. It is also a huge challenge for law-enforcement communities from different nations to coordinate their actions against cyber-crime.

The US government had launched an effort to bring different agencies together to tackle CIIP and as a result, the National Cyber Response Coordination Group was created in 2005. The group has already staged a complex nation-level exercise to map a multi-pronged attack on critical infrastructure and information systems and developed a coordinated response to this attack.

Jean-Christophe Le Toquin, Digital Integrity and Internet Safety Attorney for Microsoft EMEA, commenced by listing a number of contemporary cyber threats such as spam, phishing, spyware, malicious Code, botnets, etc.

Taking action on Botnets often provides leads in other investigations – for example, a botnet investigation leading to spammers, virus writers, etc.

Criminal uses of botnets include:

- Theft: Bots often have the ability to steal documents or data from an infected computer. Modern bots steal computer passwords, bank account numbers and passwords, and PayPal passwords.
- Piracy: A common example is the ability to steal CD keys or product activation keys from an infected computer's registry. This allows the controller to use or trade pirated commercial software with a legitimate key from a legitimate copy.
- Malicious Distributed Denial of Service (DDoS) attacks have been directed against individual sites like Microsoft (August 2003), as well as Internet infrastructure.
- Extortion: Even small botnets (a few hundred machines) can extort online businesses for money. A documented example is a small site in Kentucky that was taken down for a week because they refused to pay $10,000 (April 2004).
- Profit: Bots may include functionality that directly results in profit. One example is providing "clicks" on advertisements on web pages. Because advertisers often pay-per-click, a controller can artificially run up the click count by commanding bots in a bot network to sent HTTP requests for a particular advertisement.
- Organized crime rings using botnets.

Microsoft is fighting these threats with a network of 65 people worldwide, including 25 investigators, in addition to lawyers and paralegals dedicated to this task. The firm has also developed special Internet Safety Enforcement Programs:

- Enforcement: Coordinated enforcement programs across Internet threats including spam, phishing, spyware, and malicious code, botnets, education and awareness programs.
- Law Enforcement Partnerships – providing tools, training, technical support and child safety.

De Bruin said that the most important, yet unanswerable question is, "How big is the problem?" It is almost impossible to quantify because the numbers simply do not add up and not all parties are prepared to disclose the incidents they have encountered. Security is not just about incident response and law enforcement but also about awareness, education and preventive measures.

Other key factors for heightened cyber-security are:

- The key element for success is trust among all the actors that play a role.
- Involving the private sector is crucial because the vast majority of infrastructure and its components are in private hands. We must build public-private partnerships.
- Another challenge is cooperation at the international level. The solutions provided by countries must be compatible with one another.

Customs and Border Control

Michael T. Schmitz, Director of Compliance and Facilitation at the World Customs Organization, spoke about the challenges posed by customs and the role the WCO plays in overcoming these.

The WCO's most visible activities regarding customs and border control are within the SAFE Framework of Standards to Secure and Facilitate Global Trade. The four core elements of SAFE are:

- It harmonizes the advanced electronic cargo information requirements on inbound, outbound and transit shipments.
- Each country that has joined the framework is committed to employing a consistent risk management approach to address security threats.
- The Framework requires that at the reasonable request of the receiving nation, based upon a comparable risk-targeting methodology, the sending nation's customs administration perform an outbound inspection of high-risk containers and cargo, preferably using non-intrusive detection equipment such as large-scale X-ray machines and radiation detectors.
- The Framework defines the benefits that customs provides to businesses that meet minimal supply chain security standards and best practices.

SAFE has two pillars: the Customs-to-Customs and the Customs-to-Business pillars. Building sustainable capacity among WCO member countries is key to the implementation of the SAFE framework of standards.

SAFE is not final, but a living document that the WCO will adapt and modify as it implements the framework. As of late February 2006, 128 of the WCO's 169 member administrations had indicated their intent to implement the SAFE framework of standards.

As part of this implementation effort the WCO launched the Columbus plan in January 2006. 53 members have submitted self-assessment check lists to the WCO and 51 members will undergo diagnostic evaluations for needs assessment and development assistance.

Robert Verrue, the EU Commission's Director General of Taxation and Customs, outlined his office's vision for protecting the global supply chain, developing EU laws and regulations to facilitate this process and strengthening EU-US customs cooperation.

The EU has been progressively interested in the protection of international commercial infrastructure as the development of international logistics and new technologies has made the global supply chain more vulnerable to security threats.

WCO standards provide a model for a global solution to this problem and the European Commission fully supports the idea, in particular the instrumental role of the private sector in implementing the SAFE framework of standards. The EU and US are working very closely together to implement the SAFE framework of standards.

With the EU Taxation and Customs Union, the EU is ready to recognize the controls and risk analyses performed by the customs services of other countries. The EU is cooperating not only with the US, but also with other countries, such as China, Canada and New Zealand.

The EU is cooperating with the US on sea container security. EU and US customs authorities have also agreed to conduct joint threat assessments and to exchange liaison officers.

A key development in EU customs laws and regulations in the wake of the 9/11 attacks in the United States, including such core legislation, as Regulation 648/2005. This regulation mandates the filing of import and export declarations prior to arrival or departure. It also requires established electronic filing once the necessary IT systems are in place.

The US Customs and Border Protection's Office of International Affairs' Assistant Commissioner, **E. Keith Thomson** concentrated on the different aspects of protecting global supply chains from security threats while facilitating legitimate trade.

The WCO framework will also strengthen the Customs-to-Business partnerships in the US and the US has already advanced in this area through the Customs-Trade Partnership Against Terrorism (C-TPAT). The US looks forwards to the development and implementation of robust customs-to-business supply chain security partnership programs of equal rigor to C-TPAT by customs administrations around the world so that the idea of mutual recognition can be realized. Capacity building within the SAFE framework of standards is of critical importance and the US is working to provide assistance to countries that have requested assistance in doing so.

Reporting back on the session, **Verrue** commented that the participants recognized that customs have an important role to play in contributing to the security of the global supply chain and that close cooperation with businesses, impacted by government, essential in developing international standards in this area.

Session Five

Energy Security

Dr Armen Sarkissian, President and Chairman of Eurasia House International, Advisor to the Chairman of British Petroleum and Director of the EastWest Institute, asserted that energy security is an extremely large and complex issue before giving a brief introduction to the topic.

Global energy consumption has doubled since 1985 and many countries that were suppliers of oil have become full consumers. In 1990, China accounted for only 3.5 percent of the world's crude oil demand; in 2004 that number had grown to 9 percent, and this statistic is growing annually. India's demand for oil has also grown by 4.5 percent in the last five years while the world averaged a growth of 1.8 percent.

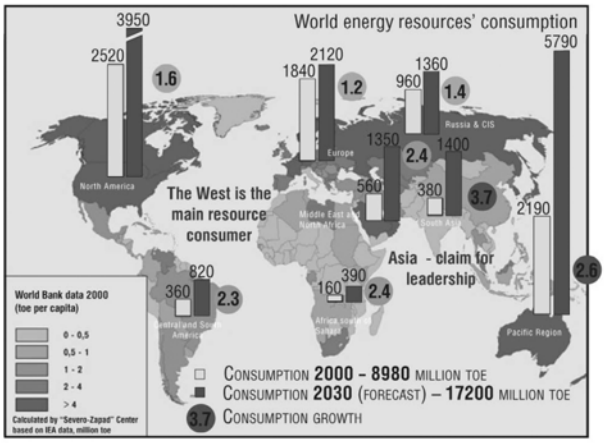
When talking about energy security, one should also look at alternative energy resources such as nuclear energy.

There are more than 25 nuclear power plants under construction, most of them in Asia. A second alternative energy could be solar energy, although the presence and development of solar energy has reduced over the last 10 years.

New reserves of oil are available, for example in Western Canada, which has approximately 170 billion barrels of extractable petrol from tar sand, but needs tremendous effort, energy, investment and new technology to make it usable.

Energy security includes the supply of oil, gas, and the effective use of all alternative energy sources. The driving forces are the growth of economies and the priority given to securing energy for the near future, including the introduction of new technologies in this field.

Dr. Evgeny P. Velikhov, President of the Kurchatov Institute's Russian Research Centre, stated that the world finds itself in an energy crisis, experienced by everyone and yet its full impact is still to be seen. One of the biggest factors in the asymmetry between supply and demand concerns gasoline. Other factors include man-made catastrophes, political problems, military conflicts, and terrorism. In order to prevent crises from occurring, a wide array of measures can be taken such as creating a more rational use of available energy as well as developing new energy sources.



World energy: Status and Trends

World energy resources' consumption
3950
2520
1.6
2120
1840
1.2
1360
960
1.4
5790
Russia & CIS
Europe
1350
2.4
1400
North America
The West is the main resource consumer
560
380
3.7
2190
Middle East and North Africa
South Asia
Asia - claim for leadership
2.6
820
360
2.3
390
160
2.4
Central and South America
Africa south of Sahara
Pacific Region
World Bank data 2000 (toe per capita)
0 - 0,5
0,5 - 1
1 - 2
2 - 4
> 4
Calculated by "Severo-Zapad" Center based on IEA data, million toe
□ Consumption 2000 – 8980 million toe
■ Consumption 2030 (forecast) – 17200 million toe
3.7 Consumption growth

Russia plays a major role in energy security, having 30 percent of the world's natural gas reserves, and 10 percent of the world's crude oil. However Russia's national economy is heavily dependent on the supply of national resources, which the country uses inefficiently – 70 percent used to generate electricity.

The aim should be to develop more efficient machinery, as well as research and development.

A correlation exists between the gross national product per capita of a country and the use of energy resources, although the proportions can change. If a country moves towards a high living standard, the use of energy also increases. This is the case in Japan and South Korea and soon to be in China and India.

Energy resources are concentrated in small regions of the world such as the Middle East and North Africa, causing the stressful situation in the market to keep growing. An increase in production is hardly possible and therefore we can expect a continuous increase in the price of oil. Energy resources are generated much more slowly than they are used.

Over the last few years, Russia has increased its production of natural gas, and, due to its strategic position between Europe and Asia, it is considering supplying natural gas to both continents as well as to North America. It will do this by utilizing the Russian Arctic Shelf, estimated to contain more than three trillion cubic meters of gas.

Russia is developing new industries that include redesigning and converting 100 nuclear submarines into production platforms for oil. These are expected to start functioning in 2007 and produce seven million tons of oil per year. The idea of underwater tankers for the safe transport of natural gas is also being developed.

However, if Russia is to act as a balancer for the world's energy supply, it will have to rethink its internal energy consumption. One scenario is to increase the use of nuclear energy at home while increasing the export of natural gas.

The obstacle to this increased nuclear energy output is the issue of technology. Russia has classical nuclear reactors and part of the debate concerns increasing the energy production in these. Old-style reactors, like the ones found in Chernobyl, are slowly being dismantled. If Russia decides to shift towards more nuclear energy, the development of these nuclear reactors will have to begin quickly or the energy production requirement will not be met. In fact, before 2030, meeting the necessary levels would require the introduction of high-temperature nuclear reactors. The development of nuclear energy will bring with it the issue of nuclear safety. The spread of nuclear energy must not equate to the spread of nuclear-proliferation and this issue must be monitored internationally.

The international community needs to diversify the production of energy in order to overcome the present systemic energy crisis. Boosting the production of nuclear energy should form part of this diversification, as it would help to stabilize the situation over the next several decades. An increase in production in Russia's nuclear power plants would also free up more gas for exportation, which would help to ensure Europe's energy security.

Christian Pibitz, Representative of the EU Security of Supply Task Force and the International Association of Oil and Gas Producers, began by explaining the role of the OGP. It is an international association of oil and gas explorers and producers, and numbers 61 companies and their associates. These members account for over half the world's oil output and approximately one-third of global gas production.

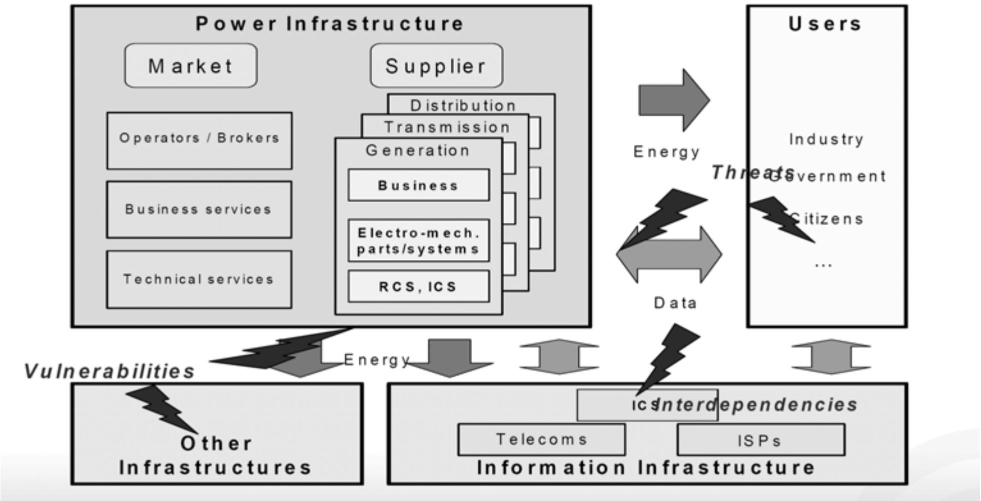
A European taskforce that includes OGP (the upstream sector) and EUROPIA (the so-called downstream part) has been formed. EUROPIA is an association of companies operating in all 25 EU countries and includes BP, Shell, Chevron and ConocoPhilips. EUROPIA is charged with representing the interests of the EU oil refining, distribution and marketing industry to European institutions.

OGP members and their contractors operate in more than 80 countries. Their operations range from front and exploration exercises in regions with little security infrastructure (the Middle East, Africa, etc.) to complex facilities in mature regions. The challenges faced by the members vary according to regions in which they operate and include trans-national terrorism, indigenous terrorist activity, and threats such as fraud, theft, sabotage, violent organized crime, civil unrest and armed conflict. These threats are managed through a combination of means, encompassing in-house security professionals, local security providers, specialist security providers and other sectors of the security industry.

The best security management is at the country level and therefore any Europe-wide approach needs to be kept flexible. OGP and the individual industry and infrastructure owners should be fully involved.

Director of Excellence on Risk and Safety Sciences at the Swiss Federal Institute of Technology, **Adrian Gheorghe's** presentation focused on energy security systems and presented intelligent action as a solution for safer and more secure energy systems.

As a result of the critical nature of energy infrastructures, it is necessary to understand demand-supply issues, environmental factors, threats and disasters that might contribute to the instability and vulnerability of such systems. There are also new dimensions to the issue like the war on terrorism and beyond. We must give thought to addressing the issues in more comprehensive ways.



When examining critical infrastructures such as oil, gas, electricity and transportation systems, huge interdependencies can be identified. Depending on the infrastructure and its interaction with others, varying degrees of vulnerability emerge. It is necessary to look at the subject in a new way. In the 1950s and 1960s reliability was critical. Over the years this has changed and today emphasis is not only placed on risk and risk management, but also on vulnerabilities, safety security, and mutual threats. This change represents a new landscape that must be addressed with new tools and adequate thought. Contemporary threats are not simple but rather multi-dimensional as they can relate to technology, politics, legislation, institutions, markets, human-induced environmental conditions, etc. and represent a web that must be addressed.

A shift is underway towards new models and ways of thinking but the specific direction is unclear.

Vladimir Orlov, Director of the PIR Center for Policy Studies in Russia, divided his presentation into three segments.

The first segment focused on Russia as a stabilizer of world energy security given its geopolitical situation and its vast resources of oil and natural gas. Russia plans to actively participate in the global natural gas market. In the future, there will not only be the transportation of natural gas through pipelines, but also the transportation of liquefied gas. With positive international cooperation this market could develop on a truly global scale. Russia has a number of gas production sites that could become additional sources for the world's energy markets. One site alone has the potential to start operations in 2010 and could produce up to 70-90 billion cubic meters of gas per year.

To facilitate this, international consortiums would be used to develop the North-European Gas Pipeline (NEGP) through the Baltic Sea. The ultimate objective is to secure an additional supply of energy.

Forecasts that suggest the possibility of reducing the use of oil and gas in the next 50 years are implausible as there will be a growing market for oil and gas in the next 10 years. Russia predicts that gas consumption will, however, exceed oil consumption by at least 2.5 percent. By working towards a global supply of gas, Russia would intend to supply gas to the whole world, not just to the regions where the pipelines led.

Russia has also been developing a policy with regard to energy security for the whole world. There are several weak spots among them Central Asia and the Caspian Sea. In the former the governments of Tajikistan, Turkmenistan, Kyrgyzstan, and Uzbekistan have to tackle growing inter-ethnic, socio-economic and other problems and dilemmas and this creates difficulties in securing and managing borders among the region’s neighbors.

Russia’s primary challenge in the region is the development of a complex strategy of relations with its governments aimed at achieving long-term stability in the region. This requires the increase and maintenance of Russian political and economic presence in the region. The 35-year contract between Russia and Uzbekistan that permits Gazprom to develop natural gas drilling locations is an example of the latter. Russia will also increase its military presence in the region in the framework of collective security arrangements.

Russia also intends to act as a guarantor of energy security. Such a role requires Russia to notice the growing competition over influence in the Middle East region around the Caspian Sea and the competition over energy resources in Iran and the Persian Gulf in general, as well as the Gulf of Guinea. The destabilization around Iran presents a serious challenge and Russia is working closely with Iran on this issue. As a possible solution Russia has promoted the idea of international centers for uranium enrichment, one of them in Russia with the possible participation of Iran, Kazakhstan, Uzbekistan and some other countries. Russia has also increased cooperation with other countries in the Persian Gulf.

LukOil and TransGaz have become involved in Saudi Arabia as a result of new agreements and Transgaz has also created a new network of gas distribution around the Gulf of Guinea.

In addition to this expansive activity in the energy markets, Russia intends to continue to develop strong international cooperation on all energy security issues. Russia has dedicated its 2006 G8-presidency to being the year of energy security.

Special Session

Public-Private Partnerships for Counter-Terrorism

Russell recalled how after 9/11, the private sector was relegated to the sidelines as governments and international organizations selectively brought business into limited cooperation, either as sources of technology, or for capital, and how a partnership was certainly not in existence.

Since then progress has been made in public-private cooperation and the Russian promotion of public-private cooperation in counter-terrorism represented a new and important opportunity.

As 80 percent of the world's critical infrastructure is in private hands, the interconnectedness of the globalized world highlights the importance of cooperation, information exchange and trust between government and business. Quite simply, it is unthinkable for the two parties not to cooperate if an effective level of security is to be reached.

Safonov explained the Russian initiative and his vision for greater cooperation between the public and private sectors.

The ideology behind Russia's initiative is simply that the business world is a natural ally of public authorities in confronting terrorist ambitions, in safeguarding the economy from terrorist threats, and in maintaining stability. Business people are some of the most active, vigorous, and independent actors in social and public processes, proactive participants in solving many practical issues of modern life, and therefore ideal candidates to take a leading role in securing our peoples and homelands.

Public-private partnerships have not however flourished probably due to a lack of mutual trust and understanding and poor coordination with respect to achieving an essentially common goal of terrorism prevention.

Russia’s paper constitutes a draft strategy on Public-Private Partnerships for Counter-Terrorism and an attempt to formulate principles and views that can be supported by both governments and the business community at the national and international levels.

The proposal deals with both existing and potential partnerships for counter-terrorism whether the exchange of information or to initiate joint counter-terror activities. Those projects and fields that would allow governments and business community to reach meaningful results have been given greater attention (the spheres of transport, critical infrastructure and the financial sector where both parties have a strong interest).

Importantly, there has been a notable interest on the part of states and businesses, and Safonov expressed his hope that the deliberations of the off-the-record sessions focusing on various aspects of the draft would provide the opportunity to gather comments and suggestions on this initiative.

The ultimate goal of the initiative for 2006 is to develop a solid, modern and meaningful Charter for public-business counter-terrorism partnerships to be adopted at a representative forum in Moscow in November 2006, and thus to initiate an independent international process of counter-terrorism partnership between states and the business community.

Franco Frattini, Vice President of the European Commission and Commissioner for Justice Freedom and Security, also drew attention to the need for public-private partnerships and to set out the key factors in this cooperation.

The European Commission has sought to intensify public-private cooperation in order to bridge the gap between the two sectors. Progress has been made and two major public -private events have taken place in the last year in addition to the business community being involved in the creation of a European Program for critical infrastructure protection.
The private sector’s involvement in security is not a novel concept as it has been protecting itself against crime for many years.

What is required is a level playing field for the public and private sectors but this will be difficult to create. The Commission intends to invest large sums into security research. Commencing in 2007 it is planned that €250 million a year will be spent on financing research in areas such as the protection of energy infrastructures, local transportation, aviation security and other key infrastructure. Much of this will go to the private sector, which is often more advanced in these studies.

Three factors have to be considered – the first being price. Many of the security tools that the private sector manufactures are too expensive for mass use.

The second issue is “versatility.” Quite simply business has to adapt its products to the needs of governments. Technological solutions must be effective and suited to the task and operations in the field.

The final key factor, which might determine the future of business in these areas, is that of the protection of privacy rights, data and fundamental rights and guarantees. If these inalienable rights and safeguards are not considered in the development of new technological solutions, partnerships will fail.

If these challenges can be overcome, both businesses and governments will benefit and security will be enhanced. This strong commitment from both sectors is necessary.

László Kovacs, European Commissioner of Taxation and Customs Union, elaborated on the role of customs in cooperation with economic operators in the struggle against terrorism.

The border control of persons and goods is a vital instruments vital in the fight against terrorism.

Customs in Europe have a significant history of working with the private sector that dates back to the creation of the Customs Union in 1968. Since then provisions have existed for simplified procedures granted to reliable traders who can benefit from the speedy release of goods. Resultantly, in the customs arena a relationship of mutual trust, common understanding and recognition of respective roles already exists.

The role of customs has evolved in recent years from collecting duties and taxes to facilitating legitimate trade and addressing the threats emerging from the rapidly growing movements of goods that might affect citizens and the environment. With this shift a significant challenge has risen: balancing the facilitation of trade while simultaneously clamping down on threats.

Customs are the first line of defense against terrorism and they play a crucial role.

The expertise of customs in controlling goods, applying modern IT systems and conducting efficient risk assessments to target high-risk consignments is essential and this is linked to their ability to cooperate and coordinate with other law enforcement authorities, such as border guards and police forces, with transport security agencies and also with the private sector.

Customs are also active in the fight against financing terrorism, as the responsibility to control cross-border cash flows and also to act against counterfeit and piracy lies with them. Kovacs gave the worrying statistic that the confiscation of faked goods by European Customs increased by 1000 percent between 1998 and 2004. These goods are produced on an industrial scale, and include medicines and edibles thereby posing a dramatic threat to the health and lives of citizens.

The EU has taken legal steps – the Security Amendments to the Customs Code, adopted in April 2005 – to handle the difficult task of simultaneously increasing security and facilitating trade. This legislation:

- Requires traders to provide customs authorities with information on goods electronically prior to import to or export from the EU (Pre-Arrival/Pre-Departure Declarations);
- Provides reliable traders with trade facilitation measures (creation of an Authorized Economic Operator – AEO - concept); and
- Has introduced a mechanism for setting uniform Community risk-selection criteria supported by computerized systems (risk management framework).

The Commission has also recently adopted proposals on a simplified and modernized customs code and on electronic customs. E-customs, he continued, provided for more efficient communication between customs administrations, and between customs and other law enforcement authorities and businesses. The challenge is to find a system that is interoperable by all 25 member states, and can further secure the supply chain by incorporating means like "e-seals" and "smart containers."

E-customs provides for computerized risk management systems that would enable authorities to target high-risk shipments, while permitting non-risk consignments to be released faster. Through electronic identification, resources can be more efficiently used to better control suspicious goods, and to achieve the instant release of all compliant goods upon their arrival at customs offices.

The international goals for the European Commission regarding customs are: mutual recognition and reciprocity of security controls and standards as well as of business partnership programs to avoid unjustified costs on business and the needless diversion of scarce customs resources away from high-risk areas.

In order to formulate an adequate response to the challenges the international community faces, close cooperation between trading partners and the private sector is an absolute prerequisite. It is also imperative to ensure the security of citizens, to provide a safe environment and to maintain the competitiveness of our economies.

Off-the-Record Break-out Sessions

Three off-the-record breakout groups discussed Russia's new initiative to build Public-Private Partnerships to Counter-Terrorism. The groups focused on: Media, co-chaired by **Cattaui** and **Vladimir Andreev**, Deputy Director of the Department on New Challenges and Threats of the Ministry of Foreign Affairs of the Russian Federation; transport, chaired by **Daniel Bautista**, EWI's Global Security Program Manager; and the financial sector, chaired by **Hudak**. The sessions resulted in constructive suggestions for improvement.

Safonov noted that work would progress on the document in preparation for the conference to be held in Moscow in November. EWI would continue to work with the Russian government and the G8 as a secretariat for a number of working groups, focusing cyber-security, energy security, and the cross border movement of goods, people and capital.

Conclusion

Russell thanked the participants for the impressive exchange of ideas between the public and private sectors and offered some examples of action by the private sector in the field of counter-terrorism, citing the collaborative efforts of the Koordinierter Sanitaetsdienst (KSD) and SAP, JSC and the Russian Federation, Iraq and General Electric, and Sun Microsystems and the Russian Federation.

Mroz thanked EWI's partner, the World Customs Organization, and summarized the recommendations for enhancing the conference's global character. These included the participation of nations from the Middle East and a more comprehensive agenda with a focus on the root causes of terrorism.

Finally, Mroz stated that the conference highlighted the effectiveness of cooperation and dialogue, and that increasingly public-private partnerships are being developed. He thanked the participants and invited them to attend the Fourth Annual Worldwide Security Conference, which will be held on February 20-22, 2007 at the World Customs Organization's Headquarters in Brussels.

Speakers

Ian Abbott, Chief of the Policy and Planning Division of the EU Military Staff
Jose Manuel Durao Barroso, President, European Commission
Walter Boerman, VP of Corporate Export Controls and Supply Chain Security, Philips International
Scott Boylan, Director for Government Affairs, General Electric Security
John O. Brennan, President and CEO, Analysis Corporation
Kim Campbell, Secretary-General, Club of Madrid; Former Prime Minister of Canada
Maria L. Cattaui, Former Secretary General, International Chamber of Commerce
Michel Danet, Secretary-General, World Customs Organization
Ronald de Bruin, Head of the Cooperation and Support Department, European Network and Information Security Agency (ENISA)
Herman de Croo, President, Belgian House of Representatives
Ricardo de Rituerto, Correspondent, *El Pais*
Gijs de Vries, Counter-Terrorism Coordinator, European Union
Carsten Fausbøll, Director of Civil Emergency Planning, NATO Headquarters
Franco Frattini, Vice-President of the European Commission and Commissioner for Justice Freedom and Security

Walter Gehr, Project Coordinator, Terrorism Prevention Branch for the United Nations' Office on Drugs and Crimes
Adrian Gheorghe, Director of Excellence on Risk and Safety Sciences at the Swiss Federal Institute of Technology
Mathieu Gorge, Head of IT security consultancy, Vigitrust
Jan Grauls, Ambassador and President, Belgian Ministry of Foreign Affairs
C. Boyden Gray, US Ambassador, European Union
Peter Gridling, Director, Counter-Terrorism Unit, Europol
Hans Tino Hanssen, Director, Protocol (Denmark)
Vasil Hudak, Vice President and Director of the Brussels Center, EastWest Institute
Gao Jian, Director-General of Security, People's Republic of China's Foreign Ministry
Rey Koslowski, Director of Research program on Border Control and Homeland Security, University of Albany
László Kovacs, European Commissioner, Taxation and Customs Union, European Commission
Jean-Christophe Le Toquin, Digital Integrity and Internet Safety Attorney, Microsoft EMEA
Fabio Marini, Head of Unit for the Fight Against Economic, Financial and Cyber Crime, DG Justice, Freedom and Security, European Commission
Rutsel Silvestre J. Martha, General Counsel, Office of Legal Affairs, Interpol
Stephen McGibbon, Senior Director, EMEA Technology Office; Chief Technology Officer for Eastern Europe, Microsoft
Kunio Mikuriya, Deputy Secretary General, World Customs Organization
Jesus Mora, Coordinator for Security and Counter-Terrorism, City of Madrid (Spain)
John Edwin Mroz, Founder, President and CEO, EastWest Institute
Boris Mylnikov, Head of the Anti-Terrorist Center, Commonwealth of Independent States
Vladimir Norov, Uzbekistan Minister of Foreign Affairs
Sean O'Brien, Industry Director for Public Security (EMEA), SAP
Vladimir Orlov, Director, PIR Center for Policy Studies in Russia
Chris Painter, Chair, Hi-Tech Crime Subgroup, Group of Eight
Ana Palacio, Former Spanish Foreign Minister; Co-Chairman, EastWest Institute; Trustee, Carnegie Corporation of New York
Christian Pibitz, Representative, EU Security of Supply Task Force and the International Association of Oil and Gas Producers
Evgeni Primakov, President of the Chamber of Commerce and Industry of the Russian Federation.
Andreas Prufert, Secretary General, EUROMIL
John Raven, Advisor, The International Air Cargo Association (TIACA) and the Business Alliance for Secure Commerce (BASC)
George Russell Jr., Chairman Emeritus, Russell Investment Group and Russell 20-20; Co-Chairman, EastWest Institute
Anatoly Safonov, Special Representative of the President of the Russian Federation for International Cooperation in the Fight Against Terrorism and Transnational Organized Crime
Armen Sarkissian, President and Chairman, Eurasia House International; Advisor to the Chairman, British Petroleum; Director, EastWest Institute
Michael T. Schmitz, Director of Compliance and Facilitation, World Customs Organization
Jamie Shea, Director of Policy Planning, Private Office of the Secretary General of NATO

Lu Shimin, Deputy Director-General, Beijing Public Security Bureau; Director of the Security Department, Beijing Organizing Committee for the 2008 Olympic Games
Matthias Sonn, Director of Germany's Task Force on International Cooperation in Combating Terrorism, Federal Republic of Germany
Max Snijder, CEO, European Biometric Forum
Gérard Stoudmann, Director, Geneva Center for Security Policy
E. Keith Thomson, Assistant Commissioner, Office of International Affairs, United States Customs and Border Protection
Valery Tikhonov, Vice Governor, Saint Petersburg (Russia)
Frank Urbancic, Principal Deputy Coordinator, Office of the Coordinator for Counterterrorism, US Department of State
Nicholas H.E. van Helten, Independent Advisor, Law Enforcement and Security Consultant
Valery Vinogradov, Vice Mayor, Moscow (Russia)
Evgeny P. Velikhov, President, Russian Research Centre, Kurchatov Institute
Robert Verrue, Director General of Taxation and Customs, European Union Commission
Antonio Vitorino, Former Commissioner for Justice and Home Affairs, European Commission
Aldwin Wight, Vice President for Strategic Development, Kroll Security Group
Alexander Zherikov, Head of the Federal Customs Service, Russian Federation

Editorial Team

Editors	William Boyd and Erol Hofmans
Photographer	Frédéric Remouchamps

For more information, please visit, http://wsc.ewi.info.