EastWest Institute

Bridging Divides

CONFERENCE REPORT

SECOND ANNUAL

WORLDWIDE SECURITY CONFERENCE





Protecting People and Infrastructure: Achievements, Failures and Future Tasks

Brussels, 7-8 February 2005

EastWest Institute

IN COOPERATION WITH

Microsoft

World Customs Organization
Organisation Mondiale des Douanes

EASTWEST INSTITUTE

Bridging Divides

EastWest Institute – Global Security Program

The Global Security Program is home to a number of initiatives that address priority security challenges facing the United States, Europe, and Eurasia and the Middle East. Our programmatic initiatives foster innovation and cooperation that forms a long-lasting foundation for a new 21st Century security agenda, maximizes the potential for prosperity, and spreads free market-democratic values. High-level working groups – whose memberships are comprised of private sector leaders and public officials, including parliamentarians, experts and representatives of relevant international bodies – help to promote a truly global security dialogue on the most pressing 21st century security challenges, from international terrorism to the spread of infectious disease.

The understanding of security and the perceptions of threats have changed in recent years, and the cooperation of the international community is more decisive than ever. International terrorism destabilizes countries and societies and is transforming domestic security. Therefore, the protection of citizens as well as of the common supply chain and infrastructure remains a core issue of the common security agenda.

The daily work environment comprises a diversity of transactions across the world's trade routes and trading partners. Policies, practices and work instruments must be robust and adaptive to function across the full range of these relationships. A large proportion of the world's business transactions are conducted through digital channels; so that technology is a basic partner of security related issues. With the increased use and reliance on technology, online security has become a primary concern of governments and businesses alike.

For more information, please contact:

Vasil Hudak
Vice President for Programs &
EWI Brussels Centre Director
87 Rue Royale, B-1000 Brussels
Tel: +32 (0)2 209 05 23
Fax: +32 (0)2 209 05 29
vhudak@ewi.info

Daniel Bautista
Program Manager
Global Security Program
87 Rue Royale, B-1000 Brussels
Tel: +32 (0)2 209 05 21
Fax: +32 (0)2 209 05 29
dbautista@ewi.info

SECOND ANNUAL
WORLDWIDE SECURITY CONFERENCE

Protecting People and Infrastructure:
Achievements, Failures and Future Tasks

WORLD CUSTOMS ORGANIZATION HEADQUARTERS – BRUSSELS

7-8 FEBRUARY 2005

BY THE

EASTWEST INSTITUTE

BRUSSELS CENTRE

TABLE OF CONTENTS

WELCOME BY JOHN EDWIN MROZ

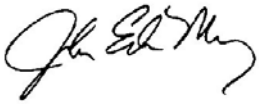
Dear friends,

As a European-American "think and do tank", the EWI is committed to an action agenda of strengthening international peace and security and addressing the critical challenges that we face in the 21st century. This *Second Annual Worldwide Security Conference* is part of a larger program, which works on global security and is headquartered at our EWI Brussels Centre.

The year 2004 witnessed important geopolitical developments in the world. At the same time, the challenges posed by international terrorism and organized crime have become more serious than they have ever been. Dealing effectively with these challenges requires close cooperation between countries and sectors. With regard to broadening effective international cooperation against international terrorism we need to extend the firm basis of European-American cooperation towards Eurasia and the Middle East. Countries that are major transit centers and frontline states in the fight against terrorism are critical to our common success. Furthermore, we have to deepen the dialogue between the sectors, namely between governments, international organizations, business and the civil society. All need to be included in the international dialogue and were represented at EWI's *Second Annual Worldwide Security Conference*.

Fostering the transatlantic and international cooperation, we must rethink how we approach borders across the globe. Our goal must be to define new ways of strengthening borders so that they both better protect our citizens and our states against threats while improving the flow of goods and people. The EastWest Institute has been working together with the World Customs Organization for a number of years resulting in the WCO hosting this year's Worldwide Security Conference at their venue.

The EastWest Institute's Centre for Border Cooperation is here in Brussels and has been working with the European Union and the Stability Pact to develop a new concept of integrated border management in the South Eastern European states area. Today there is a firm basis in European-American cooperation allowing us to have a firm foundation upon which to build. The EWI Global Security Program is committed to develop new concepts and to share knowledge with others in order to contribute to worldwide security.



John Edwin Mroz
President and CEO
EastWest Institute

INTRODUCTION BY VASIL HUDAK

Dear friends,

In the following pages, you will find the report of the *Second Annual Worldwide Security Conference*. The EastWest Institute as a "think and do tank" defined the mission of the Global Security Program, which organized the conference, as a catalyst for broadening and deepening international cooperation to protect citizens, critical infrastructure and economies against the threat of international terrorism.

Planning this conference, we wanted to achieve several goals. The first was to broaden and deepen the discussion on how to protect people, critical infrastructure and economy against terrorist threats. By broadening the dialogue, we meant going beyond only the West. The discussion is often focused on cooperation between the United States and the European Union, but we learned that security could not be divided. It is a worldwide security and the world is interdependent, requiring joint action. Having responses from Central Asia, from the Caucasian republics, from Russia was a very important element, which enriched this conference.

By deepening of the discussion we meant promoting a cross-sectoral approach to dealing with these threats of international terrorism. The dialogue and cooperation between governments, businesses and civil society actors are critical in developing an effective response to international terrorism.

We are dealing with asymmetric network-based threats, and those threats require asymmetric and network-based responses. We have to find responses which are much more fluid, flexible and quick, and which go beyond national borders. Those have to be built on international partnerships, including governments, businesses and civil associations among the key actors in the West like the United States and the European Union as well as in the Russian Federation and other members of the international community.

The EastWest Institute will continue to broaden and deepen the dialogue between international organizations, governments and civil society to contribute to strong cooperation and continuous global threat assessment.

With warm regards,

Vasil Hudak
Vice President and Director of the Brussels Centre
EastWest Institute

ABOUT THE CONFERENCE

The EastWest Institute (EWI), in cooperation with the World Customs Organization and Microsoft, organised the *Second Annual Worldwide Security Conference.* The World Customs Organization Headquarters in Brussels was the venue for this event.

The *Worldwide Security Conference* is now an annual event that examines the problems of homeland security and justice and home affairs on both sides of the Atlantic and Eurasia. This year's conference focussed on the protection of people and infrastructure, the achievements and weaknesses, and the future steps to be taken.

Around 350 business leaders, government officials and representatives of civil society attended the conference. They contributed ideas, exchanged views and provided examples as to how society was being made secure – or where work was still to be done - against the threats posed by transnational terrorism.

EWI President & CEO **John Edwin Mroz**, World Customs Organization Secretary General **Michel Danet** and the Belgian House of Representatives President **Herman De Croo** opened the conference with Secretary General of the Council of the EU, High Representative for the Common Foreign and Security Policy **Javier Solana** presenting the keynote speech.

THE CONFERENCE PROGRAM

FIRST DAY

FIRST SESSION: THREAT ASSESSMENT: COMMON THREATS, COMMON SOLUTIONS?

Pravin Gordhan, Chairman, World Customs Organization Council, moderated the first session. This looked at the international actors' perceptions of key security threats and assessed responses to those threats. Questions examined, included:

- How were the leaders of Europe, Russia, the US and their partners assessing the common security threats?
- Were Europe, Russia and the US exposed to the same degree of terrorism threat?
- How was international terrorism transforming the domestic security agendas?
- In which security sectors were countries already cooperating and where was further international cooperation mostly required?

The speakers were: **Detlef Eckert**, Chief Security Strategist, Microsoft EMEA, **Jamie P. Shea,** Deputy Assistant Secretary General for External Relations, Public Diplomacy Division, NATO and **William Shapcott**, Director, Joint Situation Center, Council of the EU.

SECOND SESSION: PROTECTING CITIZENS

The session examined international terrorism as it was being used to threaten citizens in order to destabilise countries and societies. It was assumed that protecting citizens

effectively against the threats of bio-terrorism required close collaboration between governments and business community. Questions asked included:

- Was there any cooperation between Europe, Russia and the US on how to better protect people against security threats?
- Was it realistic to fear a bio-terrorist attack?
- How were we making protection against security threats compatible with citizens' fundamental freedoms and rights?

Antonio Vitorino, Former EU Commissioner, moderated and the speakers were **Jonathan Faull**, Director General, Justice, Freedom and Security, European Commission, **Mark Chandler,** Chairman and CEO, Rules Based Medicine Inc., **László Salgó,** Assistant Director, Serious Crime Department, EUROPOL, **Annalisa Giannella**, Personal Representative of the High Representative for Matters of non-Proliferation, Council of the EU and **George Poste**, Director, The Biodesign Institute at Arizona State University.

THIRD SESSION – SECURING THE SUPPLY CHAIN AND INFRASTRUCTURE

Moderated by **Jouko Lempiäinen**, Director, Compliance & Trade Facilitation, World Customs Organization, the speakers on this topic were: **Jean Trestour,** Acting Director, Security Directorate, DG Energy and Transport, European Commission, **Andrei Konoplyanik,** Deputy Secretary General, Energy Charter Secretariat, **Brian Bjordal,** CEO, Gassco AS, **Alfons Guinier,** Secretary General, European Community Shipowners' Associations, **Wim Lintermans,** Director, GE Security EMEA and **Geoff Sawyer**, Vice-Chair, ASD Security Committee, EADS Space, Aerospace and Defence Industries Association.

The session examined one of the most urgent security issues, one that spans international economic security and environmental security as well as traditional concepts of national security. A serious breach in the supply chain could kill people, destroy goods and infrastructure, inflict significant damage on the environment and possibly trigger wider conflict. The session examined the challenge of securing global supply chains and protecting critical infrastructures.

FOURTH SESSION – TECHNOLOGY: A TOOL FOR BETTER SECURITY?

While it is well known that terrorists invest time and resources in finding new ways to perpetrate their acts through more sophisticated and devastating means, R&D is also a unique key for better security through the application of technological innovations. The session asked some key questions:

- Was technology becoming the best possible partner for security?
- What was the role of the information network in homeland security?

Chaired by Roland Schenkel, Director General, Joint Research Centre, European Commission, speakers were: **Scott Charney,** Vice President, Trustworthy Computing, Microsoft**, Bill McGann**, Chief Technology Officer, GE Infrastructure, **Zoë Baird,** President, Markle Foundation and **Robert Verrue**, Director-General, Taxation & Customs Union, European Commission.

SECOND DAY

FIRST SESSION – BORDER MANAGEMENT

The second day kicked off with a look at another key sector - border management. The aim has been to optimise efficiency and security through collaboration within and between border control agencies, together with information sharing and gradual harmonisation of procedures between neighbouring countries. The final target remains an integrated border management system. The session looked at progress in the sector and asked:

- How could countries better cooperate to increase effectiveness of border control?
- What were the best practices in use?
- What methods could be used to avoid the creation of new divisions, a wider trade gap and the movement of people due to borders being more tightly secured?

Sasha Havlicek, Senior Director, EWI Centre for Border Cooperation, was in charge of this one and she was assisted by: **Michael T. Schmitz,** Assistant Commissioner of U.S. Customs for the Office of Regulations and Rulings, US Department of Homeland Security, **Ambassador Lamberto Zannier**, Director, Conflict Prevention Centre, OSCE, **Tlegen Suntayv**, Deputy Chairman of the Customs Control Committee, Ministry of Finance of Kazakhstan and **Vyacheslav Kasimov**, Director of the Executive Committee, Regional Anti-Terrorist Structure, Shanghai Cooperation Organisation (SCO).

BREAK-OUT GROUPS

The next step was the formation of break-out groups that allowed in-depth discussion on three major topics. Each break-out group included a mixture of practical presentations and discussion, led by experts in the respective fields. The groups focussed on three areas:

- Health Security & NBCR Threats

Chair: **Ian Abbott,** Chief of Policy and Planning Division, European Union Military Staff, aided by **Jill Dekker-Bellamy,** Bio-Defence Consultant, New Defence Agenda.

- Freedom & Security

Chair**: John Richardson,** Chief Executive, European Foundation Centre, with contributions from: **James Steinberg**, Vice President and Director, Foreign Policy Studies, the Brookings Institution and **Stefaan Verhulst,** Chief of Research, Markle Foundation.

- Web-Industries and Cyber-Security

Chair: **Boaz Gelbord**, Senior Security Expert, TNO Information and Communication Technology, with a presentation (showing a commercial application of modern GPS and GPRS data communication tools enhancing security and financial returns in logistics and transportation) from **R. Fenton-May,** Chairman, Carrierweb.

FINAL SESSION: POLITICS, STRATEGY AND THE ROAD AHEAD

The final session looked back at the discussions of the previous two days and drew conclusions. Possible future actions that were put to the panel, included:

- Which were the political steps that the EU, the US and Eurasia should take to better enhance domestic security and international security?
- Could a "trilateral" strategy be agreed upon?
- What were the next steps to be considered by all partners?

Former President of Finland, and Co-Chairman of the Board of Directors of the EastWest Institute, **Martti Ahtisaari** was in charge of the final panel. It included summaries of the break-out groups by the three chairs and concluding remarks were presented by **Ana Palacio**, Chairwoman, Joint Committee of the two Houses for European Affairs at the Spanish Parliament, **George Russell**, Co-Chairman of the Board of Directors of the EastWest Institute, and **Vasil Hudak,** Vice President, EastWest Institute.

CONFERENCE CONCLUSIONS

The *Second Annual Worldwide Security Conference* achieved its goal of broadening and deepening the discussion on how to protect people, critical infrastructure and economy against terrorist threats. The main conclusions that can be drawn are:

ONGOING NEEDS

There is a need for establishing an ever greater international cooperation in the fight against terrorism, in the fields of both protection (defensive measures), prevention (proactive measures), and preparedness (responsive measures). At the same time, cooperation between the public and the private sector should be improved. In fighting terrorism, a balanced solution should be sought for, one that ensures both security and freedom. Because terrorism is an asymmetric and network based threat, the tools to fight it should also be asymmetric and network based. Finally, the motivation of terrorists as well as the underlying causes of terrorism should be addressed.

PROTECTION THROUGH TECHNOLOGICAL INNOVATIONS

There was overall agreement that technology is an essential tool in improving security. International initiatives to better screen both land- and sea borders for illegal activity, need to be assisted by the appropriate technology. Integrated Border Management and new measures like paperless customs (e-customs), will also need to be supported by technology. Furthermore, technological applications could help to early detect and control a threat. With regards to network security, products need to be secure by design in order to limit unauthorized access. Major private companies worldwide are developing new lines of business focusing on security-related technologies. It is critical to assure a quick transfer of new technological innovations for the public use, and to design public policies allowing such a rapid transfer.

PROTECTION AGAINST THE THREAT OF CATASTROPHIC TERRORISM

The biggest danger mankind is facing is a combination of global terrorism and weapons of mass destruction. Halting the proliferation of weapons of mass destruction needs to be carried out through both the physical protection of sensitive material, as well as export controls to ensure the equipment does not fall into the wrong hands. There are too little protective measures against biological terrorism, with the cost of manufacturing being small and the impact large. Furthermore, detection systems are expensive and could very well not detect the pathogen used in a bio-terrorist attack. Therefore, an international network of scientists needs to be set up to recommend new measures to be taken at early detection of such a threat.

PROTECTION OF TRANSPORT AND THE SUPPLY CHAIN

Several means of transport can be used both as a terrorist weapon, as happened on 11 September 2001 in New York City, or as a terrorist target, as happened in Madrid on 11 March 2004. Because of this vulnerability, the transport sector needs additional security, by legislative measures and a common approach. Coordination is needed between transport, immigration and customs in order to produce a safer transport sector. To secure the global supply chain, better regulation is needed to avoid constraints. Technological applications can help to monitor the movement of goods. Reliability is at the heart of the supply of energy. It needs to be built on systems that are diversified and distributed, so as to be least vulnerable to both short- and long-term disruptions. These systems need to be integrated in such a way that they cover the transportation from the producing fields through to the consumer market, and allow both producers, buyers, as well as citizens to understand risks and exposures. There is a strong need for improving the dialogue between the global businesses and relevant national authorities towards creating a more secure transport and supply chain.

PREVENTION THROUGH BETTER INTELLIGENCE SHARING

In comparison with the United States, the sharing of intelligence proves to be a challenge for Europe. By creating a network of trust for the sharing of information, the cooperation between intelligence services will be improved. Although one can never have full oversight, the intelligence that is available will be enhanced when it is shared, and can be sooner acted upon. This can be achieved through the establishment of fusion centers that assemble information, so that risk analyses can be conducted and threat assessments can be jointly developed. At the same time, it is critical to protect individual freedom.

PREVENTION BY NARROWING THE FOCUS

By narrowing the focus in the fight against terrorism, effectiveness can be improved. Focusing on the motivations of terrorists and the underlying causes of terrorism is one such example. By developing a strategy that addresses the problems of radicalization and recruitment into terrorist organizations, policies can be identified to combat these problems. The same narrow focus can be placed on the link between terrorism and organized crime.

PREVENTION THROUGH INTERNATIONAL COOPERATION

The implementation of bilateral and multilateral agreements, and the introduction of joint international solutions can enhance the effectiveness of international cooperation in the fight against terrorism. Monitoring the financial flows of capital through a cooperative international framework can help to disrupt the financing of terrorism. Cooperation between countries and international organizations in the modernization of the security and judicial structures, and the communication of best practices, can build the capacity needed on both sides for effective anti-terrorist measures.

IMPROVING PREPAREDNESS

There appears to be too little coherence in effectively responding when terrorism strikes. Contingency planning and consequence management in the event of a terrorist attack can be improved through better training; more cooperation between countries, international organizations and institutions; better communication with the public; and also with the assistance of technology, which can mitigate exposure and limit the number of casualties. Furthermore, it is important to better define the role of media in public education and information sharing.

PUBLIC-PRIVATE PARTNERSHIP

The progress of measures that can be taken to protect people and infrastructure will be in line with technological developments. More involvement is needed of the business community in the work of governments and international organizations for the improvement of measures in the fight against terrorism. Public-private partnerships can be established for the development of e-customs technology; for training of government officials to better protect their networks and infrastructure; and for the promotion of security research. Clear rules are needed to define the co-sharing of costs between the public and private sector, related to increased security matters.

BALANCING SECURITY AND FREEDOM

The legal framework for intelligence services should be improved, to provide for interception of communications. The information that is collected by intelligence services should be allowed to be used in court. This should be supported by a common approach in the area of data protection and data retention, to ensure that needs such as privacy are ensured. To avoid a compromise of people's rights, governmental bodies can be set up for this purpose.

INTRODUCTION & WELCOME

JOHN EDWIN MROZ – PRESIDENT & CEO, EASTWEST INSTITUTE

MICHEL DANET – SECRETARY GENERAL, WORLD CUSTOMS ORGANIZATION

HERMAN DE CROO – PRESIDENT, BELGIAN HOUSE OF REPRESENTATIVES

After opening words from the World Customs Organization's **Jouko Lempiäinen**, it was the task of EWI's President and CEO **John Edwin Mroz** to introduce the conference agenda. Looking forward to a "think and do" approach, Mroz outlined the principles and objectives of the two days. He said it was essential to:

- continue to broaden international cooperation against terrorism; Mroz added that much had changed since the first Worldwide Security Conference – with Eurasia and the Middle East now heavily involved within the EWI programme
- deepen the dialogue between the main players: business, European institutions, governments, police forces and civil society
- rethink the approach on borders; to strengthen them in order to protect citizens while allowing a free flow of trade and people

The World Customs Organization's **Michel Danet** was next to the podium, welcoming attendees to the WCO headquarters. Danet outlined the WCO's changing face, with its dual aims of *assisting legitimate trade* (in all aspects) and *protecting citizens.* He saw the new enemy as international terrorism, which "attacks democracy and aims to destabilise countries and world trade". Emphasising the need to determine the roots of terrorism, Danet called for coordination between all the players, including the necessary involvement of the private sector. Noting that many countries were reorganising their customs organisations (the US, Canada, the UK, etc.), he argued that improved cooperation with the private sector was vital if supply chains (from production to consumption) and critical infrastructures were to be protected.

The Belgian House of Representatives President **Herman De Croo** highlighted the importance of Belgium, with Brussels hosting more ambassadors (266) than Washington. De Croo added that over 1,500 international organisations were headquartered in Brussels and he explained that over 90% of Belgians had put anti-terrorism measures as the greatest priority in a recent poll. After outlining Belgium's role in the fight against security (when it held the EU's Presidency), De Croo emphasised the need for global understanding and argued for a balanced solution – one that brought both "security and freedom". This call was to be heard throughout the conference.

KEYNOTE SPEECH BY JAVIER SOLANA

SECRETARY GENERAL OF THE COUNCIL OF THE EU, HIGH REPRESENTATIVE FOR THE COMMON FOREIGN AND SECURITY POLICY

Presenting the conference's keynote speech, **Javier Solana** reminded his audience that terrorism was only one of the threats facing the world. The tragic incidence of the tsunami had shown the generosity of people as well as the force of nature, but other threats included WMD[1] proliferation, regional conflicts, civil wars and diseases – all had to be faced and defeated.

Focusing on terrorism, Solana argued the main threat was against "the nature of society" and against "freedom, democracy and the rule of law". He stressed the need for a global response to terrorism – one that encompassed partnerships between states and the business world. However, Solana insisted that the causes of terrorism must not be forgotten – as "people are not born as terrorist, they become one".

HIGHLIGHTS OF THE EU ACTIONS AGAINST TERRORISM

Moving on to the EU's actions in the fight against terrorism, Solana listed some initiatives:

- *Towards more cooperative intelligence services*: the aim was to create a real-time integrated system (sharing information between countries) that analysed terrorist threats and aided decision-making
  - Dissemination of information was crucial
  - Trust was a vital element
  - Cooperation between intelligence services was essential
- *The development of a Biometric system:* that would be required for everyone applying for a visa to enter the Schengen are – to help the identification of terrorists travelling on fake identities
- *Tactics to disrupt the terrorists' financing:* intelligence was the main tactic here as they mainly used cash couriers rather than traditional banking systems
- *A fight across borders:* bilateral agreements and wider international structures were being implemented, including the key role for the UN (in political terms) and its Counter-Terrorism Committee
- *Capacity building:* financial assistance from the EU to its new member states and to third countries, as all countries needed to be assisted in the modernisation process (police structures, judicial systems, internal security, etc.).

[1] Weapons of Mass Destruction.

FIGHTING THE CAUSES OF TERRORISM

Solana also stressed the need to develop a strategy that addressed the problems of "radicalisation and recruitment into terrorist organisations" – a "better understanding" was required together with identification of the policies that could be used to combat recruitment. Finally, Solana called for action in the areas of old and new regional conflicts, where stability was required in order to remove places of sanctuary and breeding grounds for terrorism. He saw the need to bring together players from a variety of background and nations – cooperation was the key.

QUESTIONS AND ANSWERS SESSION WITH THE HIGH REPRESENTATIVE

Success and failure

EWI Vice President **Vasil Hudak** wanted details of the EU's biggest achievements in the fight against terrorism to-date. As a complementary question, Hudak also wanted the High Representative's thoughts on failures.

Javier Solana highlighted the greater international collaboration and cooperation after 9/11 and the Madrid bomb attacks. He argued that these changes had occurred at the "speed of light" and had been global rather than European in scope. He also stressed the improvements in dealings with third countries – "an important part of the cooperative agenda". As for failures, Solana did not want to dwell on these, as the "fight against terrorism was ongoing" and he preferred to remain optimistic.

EUROPE AND THE US

Johns Hopkins University's **Loretta Bondi** asked for a preliminary update on the June 2003 transatlantic agreements. Speaking generally, Solana referred to "splendid" cooperation between the EU and the US. He explained that the aim had always been to share ideas, although there had been some "small difficulties" to be overcome.

TOWARDS FURTHER COOPERATION

Equity International's **William Loiry** wanted more information on the internal security programmes being taken in the new Member States.

Solana did not want to focus on those Member States, but rather on the steps being taken to upgrade systems in all countries that had systems that were less developed. He wanted future cooperation (police, intelligence services, etc.) to be on an equal footing. Solana also focused on the importance of cooperation within the Euro-Mediterranean Partnership[2] - information exchange, upgrading systems, etc. Referring to countries with "porous borders", Solana said that someone had to help, fund and advise these nations – and the EU was doing just that.

[2] The Euro-Mediterranean Partnership comprises 35 Members, 25 EU Member States and 10 Mediterranean Partners (Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Palestinian Authority, Syria, Tunisia and Turkey). Libya has had observer status since 1999.

THREAT ASSESSMENT: COMMON THREATS, COMMON SOLUTIONS?

World Customs Organization Council Chairman **Pravin Gordhan** took responsibility for the conference's opening session that looked at the commonality of threats and solutions. He asked the panel to focus on threat assessment and set them five challenges:

- how could society be involved?
- how could security be defined in an all-embracing way?
- how could the solutions be framed to embrace everyone?
- how could the symptoms and causes be differentiated, so that the causes received priority?
- and most importantly … how could words be translated into action, and action into cooperation?

THE INTERNET

Microsoft's EMEA Chief Security Strategist **Detlef Eckert** focused on the Internet, which was certainly "part of the critical infra-structure". It would soon have 1 billion users, and the problem was how to guarantee security while allowing information to be freely exchanged.

As an example of the impact, Eckert argued that if the business world lost access to email, no one would be able to work effectively. The loss of the Internet would have a tremendous impact on business. Linking the abuse of the Internet (spam, *phishing*[3], etc.) with activities by criminal organisations, Eckert described the use of "*botnets*"[4] – "armies of zombies" that were employed by organised crime (and possibly terrorists) to stop companies from trading. As for terrorism, the Internet could be used for propaganda, recruitment, information exchange, etc.

[3] Phishing: The act of sending email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

[4] Botnets are (home) computers infected by worms or trojans and taken over surreptitiously by hackers and brought into networks to send spam, more viruses, or launch denial of service attacks.

INDUSTRY AND ITS ROLE

Moving to the role of industry, Eckert said it had traditionally protected its own assets. However, following many privatisations, 85% of the critical infrastructure was said to be in the hands of the private sector. With computer networks and telecommunication networks being merged, Eckert said that Microsoft was building new protocols and new security into software, with "web services" becoming more and more important.

Stressing the need for industry to work with governments, Eckert described the work of the G8 Hi-Technology Crime Unit and the Council of Europe's Convention on Cybercrime, and called for more investment in international cooperation (training, equipment upgrading, etc.) and more public-private partnerships.

Jamie P. Shea, Deputy Assistant Secretary General for External Relations, Public Diplomacy Division, NATO, expressed surprise that there was such a focus on terrorism given that the actual numbers of attacks (ignoring Iraq) had dropped. He volunteered some reasons:

- *Perception:* a new breed of irrational terrorist was "working on behalf of God", with no political objectives, no negotiable demands, etc.
- *Globalisation was being used extremely effectively:* to convey mediaeval messages
- *The new terrorism was open-ended:* it was now against Israel, Christians, the US, democracy, regimes in the Middle East, modernity, etc.
- *It was a kind of franchised terrorism:* no longer limited to the *Al Qaeda model*

TERRORISM – WHAT'S IT ALL ABOUT?

Shea identified a problem: as the terrorists lacked "a finite political project", they sought to motivate their own supporters rather than convince their opponents. He therefore argued the necessity to communicate with the Muslim world at large and to do that effectively. Shea insisted it was not a war, as it was not a "noble cause" or a "war of ideas". He did not want the terrorists to be given the opportunity to change our culture, for example, Muslim students should still be allowed to go to the US to learn about democratic cultures. Shea also insisted it was not "the west versus the rest" as thousands of Muslims had been killed by terrorists.

As an aside, Shea said it was "heresy" to say that the US and European approaches to terrorism were different. He argued that shared intelligence had stopped many attacks that would have been worse than Madrid. Shea was of the opinion that cooperation with the US was effective; he acknowledged that gaps existed but they were not unbridgeable.

NATO AND TERRORISM

NATO could not be "all things to all men" and Shea listed principles to be followed:

1. Concentrate on activities that brought *added-value*
2. Focus on *counter-terrorism* and avoid putting a terrorist "label" on all actions
3. *Deliver results*, do not slacken the pace
4. Cooperate more, e.g. bring together NATO and EU consequence management activities

William Shapcott, Director, Joint Situation Center, Council of the EU, looked at the various approaches that could be taken to assessing terrorist threats. He could see three ways:

1. *Act on intelligence:* described as "somewhat haphazard" as it was impossible to reach all the data; so information was used to extrapolate – e.g. there could be attacks on these kinds of cities, etc.
2. *Get into the terrorists' minds*: this could be done by accessing the Internet, where sometimes there was a clear statement, e.g. Bin Ladin's "kill all Americans"; but the list of targets just became longer and longer
3. *Look at risk density:* e.g. a suspicion that attacks were being planned, could be speculative based on looking at various ethnic communities, which could be entirely wrong information or could lead to "loan individuals" being missed

Shapcott concluded that while all approaches had to be combined, there was no easy solution. Certainly, he could not answer the question – "what is the threat in Europe?" as there were varying factors in different countries. He recommended taking a narrower focus, looking at certain themes, e.g. the current one of recruitment & radicalisation, the strategy to be developed in the next six months, etc. This could be described as chopping the problem up into manageable chunks. It would lead to lower-level discussions, bilateral and multinational.

ASSESSING COMMON SOLUTIONS

As there was no picture of a common threat, Shapcott concluded that defining a common solution was next to impossible. He stressed the need for information exchange, but found problems despite the willingness of intelligence services to co-operate:

- Differences in the levels of capability (willingness but no capacity on one side)
- A lack of the appropriate legal framework (that would allow communications to be intercepted, for example)

On the positive side, Shapcott added that the EU was trying to spread best practices to facilitate such exchange of information. He concluded that it was possible to look at common features of threats, to conduct risk analyses, etc.

- "similar" solutions could be introduced

- "fusion centres" (bringing together information from police, customs and immigration services, etc.) were being created in several member states
- joint solutions were beginning to be seen with the cooperation of multinational organisations

QUESTIONS AND ANSWERS

PUBLIC-PRIVATE PARTNERSHIPS

Security Consultant **Nicolas Van Helten** wanted to know what the private sector was doing to facilitate counter-terrorism intelligence in ICT environments and SAIC's **Douglas Browning** wanted more information on the public-private partnerships – what were the best practices that Eckert had seen?

Detlef Eckert indicated that governments and industry were working together positively and pragmatically, and saw several examples of this:

- via cooperative training, as in education against botnets and similar threats
- by introducing technology that was "part of the solution as well as part of the threat"

Eckert also mentioned e-customs technology[5] that would introduce better controls in a usable and compatible manner, but which would also need to be secured against any attacks.

SECURITY HOLES?

Eurochambres' **Vincent Tilman** wanted to know Eckert's opinion on the main weakness in Europe's Information Society.

On the subject of security holes, Eckert spilt the industry into three sectors: technology, organisations (policies and procedures) and the human factor (education and training). Noting that the computer industry was still in its infancy, he said that investment was needed in all three areas.

BURDEN SHARING

Browning asked who would foot the bill in Europe (governments or the private sector).

[5] This was described in some detail later in the conference, see page 45.

Eckert insisted that the private sector had to invest to secure its IT systems and he confirmed that recent studies had shown that 85% of the critical infrastructure was in private hands. Going further, he called for more investment in research, so that groups like the Hi-Technology Crime Units had better equipment. He also argued that multinational companies had a responsibility to invest more than the amounts strictly necessary to defend themselves.

US - EU COOPERATION – IN PERIL?

The EPC's **Fraser Cameron** had been surprised that Shea had seen no war of ideas, as that was exactly what President Bush had described. Cameron therefore asked if there could be genuine transatlantic cooperation at this stage.

Jamie P. Shea responded that the EU and the US agreed that it was a battle for "the idea" – i.e. *democracy*. So there was no transatlantic disagreement, as both sides understood that terrorism grew out of frustration in non-democratic states.

He also insisted that there was a great deal of transatlantic cooperation, much of it was "in the shadows". This work continued during the Iraq crisis, when the US and Europe were seen to be at loggerheads. Shea looked forward to President Bush's visit to see more signs of positive cooperation, i.e. training military forces, provision of financial resources, etc.

NATO'S ROLE

Van Helten was also concerned about NATO; if there was no war on terrorism, what was NATO's role and could it supply threat assessments?

Shea repeated his notion that it was important for the alliance to concentrate on delivering results where it could, in areas such as air and port security, the development of technologies, protection of major events, etc. As for the future, Shea stressed the importance of NATO's cooperative programme with some 40 countries.

Making an important point, Shea argued that if the police forces, judicial systems, etc. could be linked together, the ensuing network could be used to fight organised crime, WMD transfers, prostitution, trafficking etc.

THE COUNCIL OF THE EU – WHAT COULD IT DO IN THE FUTURE?

As a final question, Van Helten wanted to know more about the Council of the EU's operations; when would it do more than simply produce documents?

William Shapcott saw new relationships being developed and a greater emphasis on sharing information. The Council would be assisting the policy-makers in a more precise manner and working groups would be focussed on specific problems.

WINDING UP

Pravin Gordhan could see several gaps in the strategy:

- *A common threat assessment:* that encompassed not only transatlantic thinking but also the North-South divide
  - US-EU considerations, "West versus the rest" (was that applicable?)
  - capacity gaps – both East/West and North/South
- *A new risk analysis* on the effects of globalisation – positive and negative aspects, e.g. franchise terrorism and the (abusive) use of the Internet, etc.
- More emphasis on *strategical thinking,* that understood the causes of terrorism
- *A legal framework* that combined freedom and the necessary methods to combat terrorism
- *Greater cooperation* between international institutions

Microsoft®

MICROSOFT IS DEDICATED TO HELPING NATIONAL GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS BECOME MORE SECURE

Microsoft recognizes that national governments and international organizations have vital information technology (IT) security needs and face more serious security threats than other technology users. Because the protection of their cyber infrastructure is vital to every country's national interest, national governments and international organizations rightly demand that products and systems be as secure as possible and that their data be protected against loss or unauthorized use, disclosure, or modification.

The Government Security Program (GSP) provides access to source code and technical personnel for Microsoft® Windows® and, starting now, Microsoft Office, to help national governments and international organizations assess the security of their existing systems today and build more trustworthy computing infrastructures tomorrow.

There are many reasons why national governments and international organizations must concern themselves with cyber security:
• Ensuring critical national infrastructure systems are secure (banking, communications, energy)
• Protecting the privacy of the nation's citizens
• Preventing spying on privileged communications
• Shielding national or global businesses from would-be hackers who might disable systems and steal or falsify sensitive data

In matters pertaining to national defense and the safeguarding of citizens' data, national governments and international organizations require secure computing environments. The Government Security Program provides the access, opportunity, and cooperation necessary to help governments assess the security of their computing infrastructures.

MICROSOFT'S GOVERNMENT SECURITY PROGRAM DELIVERS THREE FUNDAMENTAL BENEFITS: ACCESS, OPPORTUNITY, AND COOPERATION

The Government Security Program (GSP) is a royalty-free license grant that makes specific resources available to key public agencies of participating national governments and international organizations, thereby better enabling them to understand, design, build, deploy, and maintain secure computing environments. The GSP delivers:

OPPORTUNITY to enhance cyber security capabilities

The GSP provides national governments and international organizations with the opportunity to develop more secure computing infrastructures, with assistance from Microsoft development staff and security experts.

Specifically, government IT staff are invited to bring their security projects to Microsoft test labs in Redmond, Washington. Here, they can build and test their own security projects with input and guidance from Microsoft developers and security professionals.

COOPERATION arising from a mutually beneficial relationship of trust

The GSP is based on mutual trust and fortified through ongoing interaction, collaboration, and information exchange. The relationship of trust cultivated in the course of GSP participation serves as a solid foundation for future technical collaborations in designing, developing, and implementing an optimally secure government computing environment.

Specifically, the GSP gives national governments and international organizations the opportunity to provide direct product feedback and input into the decision-making process that influences product direction. The result is a better understanding of governments' unique needs, facilitating the development of trustworthy products that are more usable "out of the box."

ACCESS to security resources

The GSP provides national governments and international organizations with access to the source code and technical information used in developing computing architecture. This engineering-level view can help national governments and international organizations ensure that their existing systems are protected and secure.

Specifically, the GSP provides national governments and international organizations with secure online access to Windows and, now, Office source code and technical information for purposes of security audits and troubleshooting. A training program is offered to assist government developers and engineers in determining how best to review and analyze the data. Access to cryptographic code is also available, subject to U.S. export regulations.

To enroll or learn more, contact the Microsoft Government Security Program team at **GSPTeam@microsoft.com.**

PROTECTING CITIZENS

Antonio Vitorino, Former EU Commissioner, set the scene for a session that looked at the "enormous challenge" of finding a solution that not only protected civil liberties but also improved the law enforcement and security of societies. Vitorino argued that while the criticisms of civil liberties groups had not undermined the legal framework, recent decisions in the House of Lords and in US district courts had raised doubts. He concluded that the courts' voice would be louder in the coming months.

Looking at key questions, Vitorino raised the following issues:

- The need for a common approach in the sensitive area of *data protection and data retention;* there had been good cooperation with the US on the subject of the Passenger Name Record - now under scrutiny at the European Court in Luxembourg
- The need to learn lessons from the recent trial in Hamburg[6]; Vitorino wanted the legal framework to be improved so that information collected by military means could be used in court
- On the subject of potential CBRN[7] attacks, Vitorino asked if enough was being done (in terms of police cooperation to stop WMD proliferation)

This took Vitorino to a wider issue, as he asked who were the best spokespeople to raise the awareness of the public without causing concern. Methods would certainly differ within each member state, and the job could be done by, for example, the police, politicians, academics, the private sector, etc.

Jonathan Faull, Director General, Justice, Freedom and Security, European Commission, took the podium. Accentuating the need to protect citizens, Faull called for the private sector and governments to work closely together. Admitting that public-private partnerships were embryonic in this field (and that there was not enough interest in Europe in terrorist threat), Faull focussed on two essential areas:

6 Suspected Islamist terrorist Abdelghani Mzoudi was acquitted in a German court on charges of helping prepare the 9/11 terrorist attack.
7 Chemical, Biological, Radiological, Nuclear.

- the financial flows of capital; a cooperative framework was required to continue the current actions in this area
- critical infrastructure: with the majority of this being in the private sector, a correct regulatory environment was needed

Introducing the newly-formed DG of Justice, Freedom and Security, Faull declared that new techniques were being used and the directorate needed "help, support, information and advice". And Faull concluded, "Frankly, we are not getting enough help from business". He could understand business saying "what's in it for us?". However, Faull could see similarities between security and environmental issues. They could either be a burden (on business) or an opportunity to develop a new generation of products.

BURDEN SHARING

In terms of who should pay for *security*, Faull argued that governments and the private sector had to create a level playing field. Governments had to support research - more work needed to be done and greater incentives were needed to promote security research. Projects were underway in regard to the new financial perspective (2007 – 2013) with greater emphasis on security-related research.[8]

PROTECTION

On the subject of the protection of citizens against bio-terrorism and other threats, Faull insisted that it was an EU priority. It was a key part of one of President Barroso's recently announced major goals for the new European Commission – *prosperity* (the full implementation of the Lisbon Agenda), *solidarity* (growth for all) and *security*.

EU WORK-IN-PROGRESS

After describing some of the current and planned EU activities (preparedness against attacks, consequence management, protection of critical infrastructures, rapid alert mechanisms), Faull repeated his view that these programmes could not be successful unless they came under the hallmark of public-private partnerships. But Faull did not just ask for cooperation, he also wanted "entrepreneurial ideas" that could be tested in the marketplace.

[8] 1 billion Euros per year

Faull finally described the ARGUS[9] cooperative venture, whereby his DG was working with those bodies responsible for public health issues. The result would be a centrally coordinated network that dealt with the receipt and transmission of alerts. Faull added that this was an example of his DG not working in isolation. He wanted greater cooperation from all stakeholders - business was not making a large enough contribution.

Next up to the podium was **Annalisa Giannella**, Personal Representative of the High Representative for Matters of non-Proliferation, Council of the EU. She covered the Council's non-proliferation (of WMD) strategy, adopted in 2003 as part of the overall security strategy.

Giannella explained that the non-proliferation approach has been based on three factors: *prevention, effective multilateralism* and *cooperative partnerships*. Expanding on effective multilateralism, Giannella said that the idea was to globalise the current treaties on non-proliferation and disarmament, and to improve overall compliance. She explained that legally binding instruments existed in the nuclear, chemical and biological sectors, but not in regard to the actual delivery of missiles. Giannella added that stopping the proliferation of WMD depended on: a) physical protection (preventing sensitive material being stolen) and b) export controls (ensuring equipment did not fall in the wrong hands). Looking at the three types of WMD, Giannella commented:

- *Chemical weapons:* the WMD most recently used (in Japan and in the Iraq/Iran conflict); the Council was undertaking a joint action with the Organisation for the Prohibition of Chemical Weapons (OPCW) to improve treaty compliance. On a national basis, this was done by helping countries to draft legislation (practical effective multilateralism). Challenge inspections did not yet exist in the chemical field, only routine inspections were allowed.
- *Nuclear weapons:* the Nuclear Non-Proliferation Treaty (NPT) was the cornerstone of the legislation and efforts continued to get all countries to sign-up. In addition the Council wanted to globalise the "additional protocol", which provided IAEA inspectors with greater powers. Furthermore, the Council worked with the IAEA on joint programmes to: a) enhance physical protection of nuclear installations and radioactive sources, and b) stop illicit trafficking of nuclear arms.
- *Biological weapons:* here a convention existed but without a verification mechanism, as there had been serious disagreements on the "credibility of the proposed verification process". More work was needed – possibly "with business and industry".

Giannella concluded with reference to the work being done on export controls, with advice from the US, especially in regard to third countries. The EU has significant experience and expertise in this area, and there has been some success in agreeing non-proliferation clauses with third countries.

Mark Chandler, Chairman and CEO, Rules Based Medicine Inc., painted a bleak picture of the bioterror threat. Chandler explained that his company had become the "centrepiece for airborne particle detection systems in the US". Looking at the threat, he

[9] The European Commission has called for a secure general rapid alert system (ARGUS) to be created to link all specialised systems for emergencies that require action at the European level.

focussed on the gross discrepancies between the causes and the effects, the so-called asymmetric aspect:

- *Financial cost:* the costs of manufacturing biological weapons were small; the impact could be expressed in billions of dollars
- *Human cost:* a single person could wreak havoc (and easily avoid detection); thousands of people could be killed or maimed

Chandler argued that thousands of bioterror agents could be genetically manufactured, as it was extremely easy. But as you needed scientific assistance, he saw a greater threat coming from toxins (e.g. ricin) that were readily available in castor seeds. So what could be done to protect citizens against such threats?

Chandler looked at the particle detection systems that could be installed, but he saw inherent weaknesses:

- As they were *expensive:* the buildings under attack may not have installed them
- The terrorists may have used a pathogen that was *unknown to the detectors*[10]
- The attack might be introduced via water or food supplies, *i.e. non-detectable*

Chandler had more bad news. If a building was attacked, it was necessary to decide whether to raise the alarm (by which time hundreds of people might have entered and left the building, and it would lead to panic) or decide to keep people locked within the confines of the building.

And there were more problems. The anticipated cost of developing the anthrax vaccine was estimated at almost $1 billion. It was therefore obviously not feasible to spend the same amount of money on combating the 50-odd different toxins (and it would be unlikely that people would want to have 50-odd vaccinations). Chandler described this as "an arms race that we cannot win".

He recommended creating a group of scientists who would be called in to action at the first signs of detection, i.e. when large numbers of people reported unusual symptoms. The scientists would conduct forensic work to identify the virus, bacteria, toxin or gas, they might recommend quarantine, or supportive therapy might be provided. It was not a total solution – but Chandler thought it was the most effective one we had at the moment.

Europol Serious Crime Department's Assistant Director **László Salgó** moved the discussion on to the terrorist threat and the European law enforcement agencies' reaction. With suicide bombers and "Jihadist" terrorists now willing to inflict massive

[10] This is similar to the anti-virus systems (on networked computers) that must be continually updated to keep track of the latest viruses, otherwise they are useless.

damage without concern for their own lives, Salgó wanted new methods of protection. He argued that globalisation (with its removal of borders), while bringing benefits, had also increased the vulnerability of citizens and critical infrastructures alike.

Salgó argued that terrorists had avoided the use of CBRN weapons in the past as they had not possessed sufficient knowledge and they were concerned about public reaction. "The situation has changed" with terrorists no longer feeling they would lose the support of their main audience - "Umma[11]" (the Muslim community at large).

EUROPOL'S MULTI-FACETTED RESPONSE

- *The Europol Counter Terrorist Programme*
  - The EU Counter Terrorist Task Force had been reactivated, with representatives of the law enforcement and intelligence services

- *The Europol Counter Proliferation Programme*
  - In 2005, the CBRN Rapid Alert System (RAS), linked to ARGUS (the EU platform), will be launched
  - RAS will provide alerts in regard to critical infrastructure. However it is likely that ARGUS will circulate rapid alerts based on detection within the public health services; the law enforcement services will decide on resource allocation
- *EU Contingency Plan Working Group*, including the European Chief of Police task force; cooperation with the IAEA, OCPW, European Commission, etc.
- *Training in conjunction with the European Commission*, workshops will be available to national agencies

COMMUNICATION – THE KEY

Salgó explained that society had to be informed as to how they should react, especially in the wake of CBRN attacks. The key to success, he stressed, was finding a balanced approach that avoided creating panic in the community but provided the necessary information to the people. In this regard, Salgó mentioned the *EU Counter Terrorist Media Management* network, which exchanged best practices.

FURTHER COOPERATION

Stressing the need for improved communication, Salgó described the latest involvement with the US and with Russia. With the US, they had reached strategic and operational agreements, exchanged liaison officers and jointly developed threat

[11] Umma - Denotation for the community of Muslims, that is, the totality of all Muslims. The term comes from a word that simply means 'people'. But in the Holy Koran, the word is used in several senses, but it always indicates a group of people that are a part of a divine plan and salvation. (http://lexicorient.com/).

assessments. The cooperation with Russia had also included strategic agreements, while discussions concerning an exchange of experiences and best practices were ongoing.

NEW DEVELOPMENTS AND A HINT OF CAUTION

Salgó also described the growing links between the terrorists and organised crime. The financing of terrorism through drugs, people trafficking, credit card fraud, etc. was on the increase, and *Al Qaida* was thought to have links, for example, with drug trafficking in Afghanistan. Salgó concluded that the programme added up to a "comprehensive set of acts" but he stressed the need to find a balance between maintaining security and ensuring individual freedom and rights. He insisted that there could be no risk of criminalising whole sections of society or ethic groups. To this end, Europol had created a *Joint Supervisory Body* to ensure that the rights of people were not compromised, including the rights for individuals to know exactly how their personal data was being collected, stored and transmitted.

George Poste, Director, The Biodesign Institute at Arizona State University, was the final speaker in the first session. Reflecting on the "dramatic shift in public consciousness", Poste looked at the potential for bioterrorism and the causes for concern, which included:

- a deliberate targeting of civilian populations
- multiple threats, multiple targets and diverse attack scenarios
- the protracted contamination of buildings, e.g. after an anthrax attack
- public fear and the risk of civil disorder
- the low cost (of attacks) and the high cost of defence

Poste argued that while the risk of a bioterrorist attack was low, this probability would increase as the technology required to launch an attack became more readily available. Due to dual-use technology, Poste reasoned that the spectrum of attacks would increase and grow to cover "biological circuit disrupters" that could impact the human body's processes.

Expanding on the threat, Poste reasoned that the likely attacks would be low-level and continuous, and against "people, livestock and crops". This led him to his final cause for concern – "major shortcomings in governmental policies".

Poste did not waste his words and described a picture where threat assessments (G8, OECD) differed, plans were fragmented and there was "woefully inadequate international co-ordination. In the event of an attack, there was "ill-defined" consequence management planning and a lack of priorities as to who would be provided

with scarce drugs and vaccines. There was no framework for sharing information, plans or vaccines in the event of an attack.

Poste's conclusion – *there was a total lack of engagement with the private sector.*

BIOINCIDENT MANAGEMENT

In the event of a "bioincident", Poste underlined the necessity for the three main actors (the decision-makers, the public health authorities and those responsible for maintaining civil order) to be linked via effective communication networks. He added that any public pronouncements had to be made so that credibility and public trust were maintained. Dismissing the idea of a "quick-fix", Poste backed Chandler's arguments that detectors could *not* provide any sore of protection. But this was only one "false premise", and Poste had more. He argued that:

- The "B" in CBRN was totally different from other threats, the first sign of a biological attack would be stricken people or animals in torment
- Therapeutic stockpiles were inadequate, e.g. there were only 10,000 reserve respirators in the US
- No coherent disaster plans existed
- Regular drills, to rehearse action to be taken in the event of an attack were not held
- The legal aspects of keeping people in quarantine were not well understood

THE WIDER PICTURE

Poste argued that the US public health systems had been dramatically eroded in the mistaken belief that there was no need to defend against infectious diseases - either naturally occurring or otherwise. He blamed fiscal neglect, a lack of career appeal, inconsistent national policies and an ignorance of the wider picture.

Turning to the subject of biosecurity, Poste reasoned that it was much wider than bioterrorism, as it also covered the threats of infectious diseases from natural origins and environmental deterioration. To face these threats Poste wanted:

a) structured and consistent investment to rebuild the public health systems
b) more engagement with the private sector
c) international cooperation
d) commitment and political resolve

Poste had heard many fine words, for example at the "G8 Summit on Global Fund for AIDS, Malaria and TB" in Genoa in 2001, but he was still waiting for the results of those words. Industry had to be engaged, as it was obvious that the Bioshield arrangements were not working (lack of financial incentive for medical and pharmaceutical companies, no indemnification, and insufficient coverage under the Safety Act).

Poste had only negative conclusions. Planning was fragmented and resources were being wasted. He called for a systems-based approach to be taken, with biosecurity receiving a greater priority from governments, and the creation of a global infrastructure on surveillance, diagnosis and containment.

QUESTIONS AND ANSWERS

The Brooklyn Law School's **Richard Allan** wanted to know if the two sides (law enforcement and campaigners for civil liberties) were being brought together. Allan wanted ground rules to be agreed so that law enforcement officers could do their work without the need to look over their shoulders.

Jonathan Faull could never see an end to that particular discussion, as a "perfect solution" did not exist. Law enforcement services wanted information (their raw material) and others would always be watching to ensure that people's rights were not abused.

SECURING THE SUPPLY CHAIN AND INFRASTRUCTURE

The session "Securing The Supply Chain and Infrastructure" was chaired by **Jouko Lempiäinen**, Director, Compliance & Facilitation, World Customs Organization. Lempiäinen pointed out three basic risks in regard to trade infrastructure. Beginning with the means of transport being abused to carry terrorists or weapons of mass destruction, he elaborated on planes and ships which can pose a threat when they are used as weapons themselves – such as experienced at 9/11; or which can be a target for terrorist attacks, as happened in Madrid in March 2004. These different threats imply the danger of an interruption of economic trade when security measures have not been taken sufficiently.

Opening his remarks, **Jean Trestour,** Acting Director, Security Directorate, DG Energy and Transport, European Commission, noted that the Council had called for all forms of transport systems to be strengthened in the face of terrorist threats. He suggested that operators consider security as an additional quality, not just as an anti-terrorist measure. Trestour reviewed the current situation and the Commission's future plans.

MEASURES ALREADY IN PLACE IN THE EU

- *aviation:* legislation was in place at airports, there were common basic standards, inspections on a regular basis and there was a common interpretation of the Chicago convention
- *maritime legislation:* the ISPS code[12] was in place to cover domestic passenger transport and ferries, legislation was enforceable at the EU level, the compliance system had been approved and inspections were due to start; a "port security" directive was under discussion

THE EUROPEAN COMMISSION'S FORTHCOMING INITIATIVE ON SECURING THE SUPPLY CHAIN

Trestour noted that security started at the shippers' premises, so shipments had to start with secure methods in place. This was no easy problem to solve, given that there were millions of movements per day, 500,000 operators and just as many dealers and wholesalers. On the positive side, Trestour noted that many operators were introducing more secure methods, as they knew that "being secure means more business".

[12] The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks.

However, he argued that the realities of life meant that securing the supply chain was an evolutionary process. There would be no big bang, and progress would be in line with technological developments. Outlining various concepts, e.g. *the Community Customs Rule* and *the Community Airport Regulation,* Trestour said this type of voluntary compliance, once vetted, would be rewarded. A concrete proposal was being formalised, and it would be in line with the efforts of customs' authorities and the US.

SECURING THE CRITICAL INFRASTRUCTURE

- *Transport:* a study would soon be launched, including an inventory of the critical infrastructure
- *Energy:* power plants, electricity grids, transmission lines were exposed to major threats; the challenge was to determine what must be done across the EU-25

Trestour indicated that the priorities were: a) the evaluation of system vulnerabilities and b) the development of a community approach to reduce the risks of such events in view of the EU's inter-related systems. These priorities would be the subject of a study in the near future. He concluded his remarks by insisting that the work of all experts (transport, immigration and customs) had to be coordinated to produce a safer transport sector.

Andrei Konoplyanik, Deputy Secretary General, Energy Charter Secretariat, initially focused on energy security, defined as the "ability to assure adequate, sustainable supply of energy at a reasonable cost". Describing "energy security" as a process that varied over time and by location, he said that, even when achieved, it could not be guaranteed forever. It had to be maintained, by the correct allocation of resources and by making the right choices. The main factor, according to Konoplyanik, was making the right investment decisions. Looking at the situation from both *consumer,* for example the US, and *producer,* for example Russia, perspectives, he listed the different viewpoints:

- *A consumer / importer wants*
  - Higher domestic productive capacity;
  - Less dependence on imports;
  - Better ability to second-source energy in case one or more suppliers interrupt deliveries, i.e. availability of alternative sources.

- *A producer /exporter wants*
  - Lower potential shortfall in domestic "exportable" energy resources;
  - Reduction of non-renewable resources;
  - Reduction of inefficient domestic use of non-renewable resources, thus providing an alternative for increasing its export potential;
  - Lower growth in domestic energy demand, for the same reason;
  - A reduction in the potential loss of competitiveness on international markets;

He concluded that it was in the best interests of both the consumer and the producer to develop energy supply systems that are least vulnerable to both short- and long-term disruptions.

SHORT-TERM DISRUPTIONS

Terrorists might target large-scale, centralised and vulnerable systems. Interruptions may occur, as alternative supplies might be difficult to find.

LONG-TERM DISRUPTIONS

Preferring a different approach, Konoplyanik quoted Woolsey and Lovins, who had stated, "energy security starts with using less energy far more efficiently to do the same tasks. The next step is to obtain more energy from sources that are inherently invulnerable because they are dispersed, diverse, and increasingly renewable".[13] Again Konoplyanik reminded the audience on the need for investment and made two conclusions:

- *Short term:* producer and consumer countries might co-operate to reduce the vulnerability of *existing energy supply systems*, and avoid some of the cost of the failure or the damage of such systems. This type of investment, while useful and maybe even unavoidable in the short run, would have limited returns in the long run.
- *Long term:* it would be necessary to diversify energy supply sources and *build invulnerable, diversified and distributed future energy supply systems* that *could handle local disruptions with ease*

His message was that energy consumers and producers were interdependent, linked together by both energy flows and investment flows, i.e. to develop energy projects. *Securing the supply chain, in this sense, "means providing better security to investors and their investments"*. This interlinking of consumers, producers and their investors led him to declare that the right policy was one that supported *competitive global energy markets.*

The next speaker **Brian Bjordal,** CEO, Gassco AS, was the right man for the job as he was responsible for the "world's largest offshore integrated gas transport system". With $20 billion invested in transportation, and over $200 billion being invested overall, Bjordal emphasised the need to have an integrated system that covered the transportation from the producing fields through to the consumer market.

[13] R. James Woolsey, Amory B. Lovins, and L. Hunter Lovins: *Energy Security: It Takes More Than Drilling.* Web publication accessed on January 19, 2004.

The importance of Norway's energy was not overlooked, as Bjordal reported that it produced 15% of Europe's total gas consumption. He added that Norway was the third largest gas exporter after Russia and Canada.

AN INTEGRATED SYSTEM

Bjordal wanted to highlight one factor - it was vital that the system allowed everyone (producers, buyers and citizens) to understand risks and exposures. It was a complex system, but – disagreeing with some previous speakers – he said that Gassco was going further, and was now looking at accidents with low frequency estimates, i.e. "the unthinkable".

Gassco had developed new tools, conducted an analysis of the threats and brought all the methods together, including traditional risk analysis. The system was being continually updated and adjusted based on real incidents.

Bjordal stressed the advantage of having a large proportion of sub-sea pipelines, so they had natural protection (600 metres of water). He explained that one of these pipelines (34" in diameter) could produce 20% of he UK market's gas supply. As for repairs, these could be conducted under water by remote-control welding.

Bjordal summed up his remarks by stressing "reliability" (security of supply) was at the heart of the business. Risks and exposures had to be understood, and you must be prepared for surprises so contingency measures could be put into effect.

Alfons Guinier, Secretary General, European Community Shipowners' Associations, said he was speaking on behalf of the ECSA which covered the EU and Norway – the European Economic Area. The shipowners in question were covering a range of vessels, including tankers, cruise ships, ferries and cattle carriers.

A key figure for Guinier was that Europe controlled over 40% of the world fleet, much of which was working in cross-continent trade, outside of the EU. As for Europe itself, 90% of its trade was transported by sea and there were 12 million intermodal-moves (of maritime containers) per year. This was a supply chain that needed protection, although security had been a factor ahead of 9/11. Guinier underlined a number of basic points that were fundamental if security was to be improved. These included:

- Conducting a proper risk assessment (described as the "start of everything")
- Taking "proportional, relevant and cost-effective" measures
- Avoiding duplication (and Guinier felt that many speakers were duplicating efforts)
- Avoiding trade distortion by improving quality
- Avoiding the movement of responsibilities from governments to industry

- Ensuring a global approach
- Avoiding competitive distortion of trade between the different modes

SHIPPING

The ISPS (International Ship and Port Facility Security Code) existed and had been transferred to an EU Regulation – 725/2004, so a global approach was in place. The ISPS code guaranteed sound management techniques and the ship itself could be identified (AIS), tracked and was able to give alerts.

On the subject of ports, Guinier referred to an earlier presentation about the EU directive. It would be similar to the ISPS code, but for all port areas. It was described as a "pre-cursor for ship security".

SUPPLY CHAIN SECURITY

Bringing it all together, Guinier moved to the complete supply chain. He wanted all actors to play their part but he was concerned that certification schemes for operators were voluntary. EU regulation was in the pipeline but Guinier wanted more, as this was "not good enough". For maritime intermodal containers, Guinier called for a total "cargo risk assessment" to be conducted (on shippers, cargo, consignee, etc.).

The ECSA had already informed the EU authorities that they wanted a mandatory advance cargo declaration "24 hours in advance of loading" to avoid problems once the cargo was on board ship. The other key pre-requisite was intelligence – so suspicious cargoes could be identified. As for the containers themselves, there should be a mandatory sealing of containers at the shippers premises ("simple but secure").

In the meantime the US authorities have brought in CSI, C-TPAT and their own 24 Hour-Rule. Guinier commented that Europe would appreciate a system that was more advanced than C-TPAT. He added that the 24-Hour Rule should be applied in Europe, and the related "advance cargo declaration" had been recommended to the EU institutions. Importantly, he added that the introduction of the 24-Hour Rule in the US had improved the flow of information and efficiency of the supply chain.

Wim Lintermans, Director, GE Security EMEA, introduced an initiative from GE Security that provided a solution for enhancing the security of intercontinental movements of intermodal containers.

Starting with the threat, he gave a succinct overview, declaring that 90% of intercontinental trade was shipped in 19 million intermodal freight containers. 20,000 containers landed in the US every day and only between 4% and 5% were targeted for inspection. And if there was one incident, it could totally disrupt global commerce.

Explaining the importance of the supply chain to GE (over 140,000 transoceanic containers per year), Lintermans moved to the challenge, which was to produce an automated integrated global system from "stuffing to unloading", with tracing at key sub-points (such as harbours) and with information available at all points along the backbone.

In detail, the requirements included: global applicability without local regulatory constraints, installation for the lifetime of the container, affordability, deployability on existing and new containers and expandability to accommodate future sensing technologies.

Lintermans introduced GE's solution – *CommerceGuard* – that had three components:

- The container security device (CSD) itself (about the size of a hand, in the container door)
- The reader infrastructure – both hand-held and fixed
- The *CommerceGuard* backbone (where shipment data was collected and made available)

Lintermans explained that this device (*CommerceGuard*) was just the first of several to be introduced, in future, devices would be more integrated within the containers and employ more advanced sensing technologies. It would be an evolutionary process.

Lintermans finalised his presentation with recommendations, with a view to achieving global deployment of the device across a global security framework. He called for:

- the creation of meaningful incentives such as "Green lane" administration for "Smart Boxes" that used container security devices (CSDs)
- greater support for private-sector financed solutions
- the further implementation and global coordination of initiatives
    - WCO: Framework of Standards
    - US: C-TPAT, CBP "Smart Box"
    - European Commission: AEO, Modernised Customs Code (similar to the US programmes)

Speaking on behalf of the Aerospace and Defence Industries Association (ASD) Europe[14], **Geoff Sawyer**, Vice-Chair, ASD Security Committee, EADS Space, looked at how ASD was supporting the European Commission in its future security research programme.

His starting point was the European Security Research Programme (ESRP), to start in 2007. Preparatory actions were ongoing and a European Security Research Advisory Board (ESRAB) was being established. As for ASD, the organisation represented businesses with over 100 billion Euros of annual turnover, with over 600,000 direct employees.

14 ASD; formed as a result of a merger between AECMA (Aerospace Industry), EDIG (Defence Industry) and EUROSPACE (Space Industry). It represents 34 national associations in 21 countries across Europe.

In order to prepare for the European Commission research programme, ASD created a network of industries, including the Security Network for Technological Research in Europe (SeNTRE), which was selected following the Commission's tender process. Key to this work was the creation of Security Mission Industry Groups (SMIGs), composed of 220 experts (some from outside of ASD) from 86 companies/organisations and 14 nations.

SENTRE

Sawyer then moved on to SeNTRE, a strategic imitative that would aim to

- prepare, for the Commission, a strategic research plan that would define priorities for the next 10 to 15 years
- develop two interlocking networks to allow consultation between technology experts (based on SMIGs) and end-users

In essence, SeNTRE would support ESRAB and be a vital player in the definition of the ESRP. SeNTRE's methodology will start with the complete range of security missions and then select capabilities to be focussed on. Technologies would then be identified to meet the capabilities requirements, with the result being a total security R&T plan. At the end of 2005, there will be a forum held to present the study results, under the auspices of the EU Austrian presidency.

QUESTIONS & ANSWERS

SAIC's **Douglas Browning** was the first with a question, asking **Alfons Guinier** to enlarge on his comments in regard to the C-TPAT initiative and on Europe's possible initiative.

Guinier said C-TPAT had good intentions but he understood that it was not being controlled sufficiently, with a subsequent loss of added value. He was supportive of C-TPAT's objectives, and he felt a similar system might be introduced in Europe but with better controls.

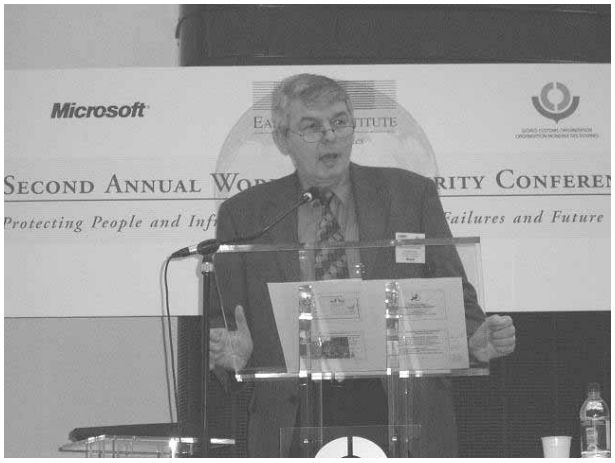
Giles Noakes of Jigsaw Container Logistics Security commented on C-TPAT, saying it suffered from a lack of incentives (this was now being addressed) and a lack of "teeth" (i.e. resources to validate the process). He wanted those lessons to be learnt in Europe. He then suggested to **Jean Trestour** that allowing market forces to act might be a bad decision when it came to introducing supply chain security – as time was of the essence.

Trestour agreed that systems had to be enforced now. Participation was voluntary, but it was the job of member states to check that registered participants were following the necessary conditions.

The Royal Institute of International Affairs' **Olivia Bosch** was concerned about; a) the possible loss of jobs (particularly in developing countries), and b) opportunities that might be missed if improved data flows unearthed corrupt practices.

Guinier did not see any job losses resulting from improvements in the supply chain. However, he could see jobs being created in line with better trade. On the subject of better information being available, he agreed that corruption might be identified earlier.

TECHNOLOGY: A TOOL FOR BETTER SECURITY?



Roland Schenkel, Director General, Joint Research Centre, European Commission chaired the final panel of the day. He prefaced the panel with a small presentation, which asked the question "Is technology a tool for better security?" In answering the question, Schenkel proffered a "Yes … but …" as there were limitations. In his presentation, he focussed on the threats against citizens, the infrastructure, the supply chain and the environment. These consisted of: terrorism, organised crime, the proliferation of WMD and the menace arising from failed states and regional conflicts.

Looking at how technology could help to fight these various threats, Schenkel gave an overview of the possibilities:

- Early detection and control; including intelligence, sensors and personal identification systems
- Engineered protection (barriers, mitigation of exposure, isolation techniques)
- Fast response (the ability to interrupt or neutralise attacks)
- Improving the fragility of targets to withstand attacks
- Forensic examination after the event (chain of evidence)

However, Schenkel reminded the conference that technology alone was not enough. There had to be human involvement in order to take advantage of experience, expertise, analytical skills and awareness of the situation (watching for unusual signals etc.)

The first panel speaker was **Scott Charney,** Vice President, Trustworthy Computing, Microsoft, who initially touched on the Internet, which he explained had been built without security – as the early users had all been trusted. Charney had also had problems early in his career when he had failed to interest many (IT and telecommunications) companies in security. That was a constant pattern until 9/11.

Describing 9/11 as an attack on capitalism, Charney highlighted one of the questions asked after the attacks - "when will the stock markets be trading again?" That moved the focus to IT systems – companies with "disaster recovery systems" and off-site redundant servers recovered faster than those that did not. Finally the markets and companies had agreed, security was important!

MICROSOFT'S APPROACH

Charney explained that Microsoft's strategy was to produce products and services that were "secure by design, secure by default and secure in deployment".

- *Secure by design:* achieved by reducing "vulnerabilities in code", developing "threat models" up-front and by developing "smart products" adhering to the "least privilege" concept – limited access unless essential need identified
- *Secure by default:* products shipped with many functions "off" to increase security
- *Secure in deployment:* achieved by providing clearer guidance (and tools) to manage products, streamlining patching mechanisms across the Microsoft range of products

Bill McGann, Chief Technology Officer, GE Infrastructure, started his remarks by venturing that "security and technology would either succeed together or fail separately". However, he agreed with Schenkel, saying that technology "was not a silver bullet". The answer was to build and design total solutions in areas such as: video surveillance, access control, intrusion detection, etc. Turning to examples where technology could provide solutions, McGann demonstrated *"millimeter-wave technology"* to track suicide bombers, *multi-scanning technology using RF waves* to identify explosives and *bio-detection systems* for the rapid detection and identification of biological and chemical threats (including field portable Raman devices).

The next speaker was **Zoë Baird,** President, Markle Foundation. Baird also looked at how technology could help security, but from a broader perspective. She focussed on a problem: how could information be identified and distributed to the people who needed to see it? And could civil liberties be protected as this was done?

A POSSIBLE APPROACH FOR EUROPE

Baird explained that, following work by the Markle Foundation Task Force on "National Security in the Information Age"; recommendations had been enacted within US legislation[15]. The Markle Foundation had suggested the creation of a trusted information-sharing environment[16], based on certain key concepts:

- A distributed network, that did not force information to the centre
- Important information was likely to be identified at the "borders" of the network
- People who would be able to make the most efficient use of data would be at the "borders"
- Information should be shared broadly around the network without erosion of civil liberties

[15] Intelligence Reform and Terrorism Prevention Act of 2004.
[16] The full report of the Markle Foundation's work is available at http://www.markle.org/

Baird emphasised the use of ICT tools in the creation of such a network, for example in limiting access to information (limited permissions) and by allowing business modelling of the way governments work. However, she stressed that "strong policies and guidelines" were essential. Such a framework had to be created at the design stage of any system / network, so that necessary features – such as the need for privacy – could be built into the overall software architecture.

A CHANGED APPROACH IN THE US

Baird concluded by recounting the way in which the US now exchanges information between its various institutions (agencies – federal, state and local; plus the private sector) so that there was more information sharing. She again emphasised the role of ICT tools and the need for privacy to be protected, especially where confidential sources existed. As an example, Baird described an eBay-like authentication tool that showed how reliable a person was in not divulging critical information, via a reliability rating.

Robert Verrue, Director-General, Taxation & Customs Union, European Commission, commented that in order for trade to be effective in the 21st century, customs departments had had to take on a new role – one that took account of risk management and facilitated trade. Taking a step back, he reminded the audience of the package of measures introduced by the Commission in 2003 that aimed towards; a) the integrated management of the EU's external borders, and b) an e-customs initiative (paperless customs)[17].

Expanding on the new role of customs, Verrue emphasised the need for a high-level of cooperation between customs and other institutions at the external frontiers if the security and safety of citizens was to be insured. To this end, the EU had set some priority actions points, in what was essentially, an *international* operation:

- The modernisation of customs legislation
- The development of an EU risk management system
- The establishment of an authorised economic operator program
- The development of the underlying IT framework

[17] http://europa.eu.int/comm/taxation_customs/customs/policy_issues/e-customs_initiative/index_en.htm

SECURITY

Verrue then took the opportunity to stress the role of the customs authorities, as they had a unique position in maintaining supply chain security, due to their complete overview of all the players and their ability to identify and control high risk situations. Essential in this operation was the development of a *risk management framework* that would safeguard trade, citizens themselves and the supply chain. Verrue called for a common approach and common standards across Member States, so that controls could be developed and targeted at those areas that posed the greatest threats to trade and personnel. Above all, he wanted a "partnership of trust".

ACCREDITATION

Moving on the Commission's concept of authorised economic operator, Verrue said its establishment was vital if the EU wanted to be a credible partner with the rest of the world. It meant that businesses (and their suppliers) would have to meet necessary standards and in return, accredited operators would not be subject to delays. This would save any unjustified costs and would also save scarce customs resources being taken away from high-risk areas.

E-CUSTOMS

Verrue also expanded on the aforementioned e-customs initiative as a basis for:

- Effective communications and information exchange between customs and industry
- The simplification of trade facilitation procedures
- Effective working methods in the areas of risk management and security-based controls
- Electronic interchange of information (internal and external to the EU)
- Data to be provided once only and then shared (single window concept)
- Goods to be controlled once (one-stop-shop concept)
- Resources to be better planned and deployed

Concluding by calling for technological applications to be developed in key areas (container integrity, high-speed data analysis, etc.) Verrue called for cooperation between the main actors (the US, the EU and Japan) to develop common requirements and common standards so that the main suppliers of technology could deliver the necessary hi-technology solutions across the board.

QUESTIONS AND ANSWERS

The BSIS's **Arthur Jacobs** had a question on threat models. He wanted to know if Microsoft was encouraging SMEs to incorporate such new techniques into their design lifecycles.

Scott Charney agreed that it had to be an industry initiative. He explained that all Microsoft's work had been published[18], and that the automated tools (to look for vulnerabilities in code) were now included in Microsoft's development platform – Digital Studio.

Summing up, Schenkel covered the key conclusions:

- In product development, security should be included at the design stage
- There were lots of opportunities for R&D developments that had to be embedded in an overall system
- Collection and information sharing had to be improved between law enforcement officers and information providers (authentication systems)
- There should be greater emphasis on risk management in the EU, backed by ICT systems and tools
- Standards for communications, requirements and solutions – were vital

[18] Threat Modeling (Microsoft Professional) by Frank Swiderski and Window Snyder. Writing Secure Code, by Michael Howard and David LeBlanc. Also see http://www.cyberpartnership.org/SDLCFULL.pdf

BORDER MANAGEMENT

Before giving the floor to the panel, **Sasha Havlicek**, Senior Director EWI Centre for Border Cooperation, introduced the topic by declaring that border management was now firmly in the spotlight. That being so, the challenge was how to find a balance between allowing freedom of movement (people and goods) and addressing the threats to both. Furthermore, there had to be a common vision between the EU, the US and those countries "on the peripheries". She was concerned that actions (described on the first day) might lead to an increasing trade gap that might even fuel terrorism.

Noting that the EU's strategy for an integrated border management system was being offered to its neighbouring countries, Havlicek welcomed the EU's closer cooperation with the US on these matters.

Looking back at last year's conference, Havlicek suggested that this was a good opportunity to see to what extent the gaps between the US and Europe (differences in approach, frustrations) had been closed in the intervening period. In addition to that, the session would be a good opportunity to understand what role the OSCE (and similar actors) could play, especially in conflict areas. Stressing that border management needed cooperation on both sides of the border, she moved to the need for greater regional cooperation (between sub-regional groups).

Michael T. Schmitz, Assistant Commissioner of U.S. Customs for the Office of Regulations and Rulings, US Department of Homeland Security, was the first speaker of the final day. Schmitz covered the background to the creation of the US Customs & Border Protection department (CBP) within the Homeland Security department, post 9/11. He argued that while certain actions were "works-in-progress", benefits had been gained: there was now one platform for border security and trade purposes ("one face at the border") and there had been better co-ordination with other international agencies.

INITIATIVES IN OPERATION SINCE 9/11

- *land borders:* the FAST procedure aimed to facilitate "free and security trade between the US, Canada and Mexico, via common risk management procedures, supply chain security, and advanced screening techniques; C-TPAT-enrolled carriers received expedited clearance via dedicated lanes and a reduced number of examinations (for approved carriers)
- *passengers – from Canada:* the NEXUS system reduced delays at the border for pre-screened low-risk passengers, via dedicated lanes and simplified procedures
- *passengers – from Mexico:* the SENTRI procedure was the first automated border control system, aiming to reduce congestion for pre-enrolled passengers
- *24-Hour Rule:* obligatory that manifest information be provided 24 hours in advance of shipment
- *Container Security Initiative (CSI):* containers reviewed at host sea ports; reciprocal arrangements had led to officers (Japan and Canada) going to US ports – described as the "only multinational system protecting shipping"
- *C-TPAT:* partners were validated for application of the minimum approved standards and best practices

However, Schmitz called for all nations to do more in regard to movements in and out of ports. He welcomed the US and EU cooperative agreement (April 2004) to spread CSI principles. Since then several measures had been adopted, including the creation of an information exchange network, a pilot project involving EU-US shipping and the exchange of liaison officers between the EU and Washington.

Schmitz concluded by adding his agreement with Verrue's comments of the previous day, and declaring that the EU and the US were "moving in the same direction". He was confident they could meet their joint "twin goals" of securing global trade and facilitating its movement.

Havlicek had just two comments. She wondered how such collaboration (on border management, and especially between law enforcement and customs) could be generated further afield – beyond the EU and the US, and also – how could the movement of low-risk cargo (which necessitated access to hi-technology solutions) be introduced without an impact on the trade gap.

Ambassador Lamberto Zannier, Director, Conflict Prevention Centre, OSCE, emphasised the increased attention being paid by the OSCE to border issues, following the increased number of conflicts and post-conflict situations. Looking back, the Ambassador described the creation of the OSCE's approach to border management and the creation of a "border unit". The first step had been to map out the activities on the ground; the results had been surprising, as many issues had already been addressed (the field employees had been

moving faster than the central OSCE staff). The OSCE's philosophy in general had been to look at soft security tools, democratic recognition and economic reforms in a number of countries.

Ambassador Zannier then gave an overview of the activities undertaken and the lessons learnt to-date.

1. *Within S.E. Europe:* cross-border cooperation between Albania and Kosovo – an example of working in an unresolved conflict area; some parts of border were not controlled by local institutions and parts of the border were still under dispute

2. *Across broader areas of S.E. Europe:* joint programmes were introduced with the aim of aiding transition and capacity building – in the context of local agreements on the ground; phase 2 (2005) would include participation in the CARDS project; overall the future was clear as there was an EU perspective with the majority of countries aiming at EU standards

3. *Further east - Moldova:* less clear, there were existing conflicts, discussions ongoing with Ukrainian officials in relations to customs controls; the EU was also providing border services including the provision of sophisticated equipment

4. *Further east – Georgia:* one of largest border monitoring operation at the OSCE, on the Georgia – Russia border, helping the Georgian border guards to monitor traffic and also to stabilise the capacity of the border services (in a volatile situation)

    a. *There was a need for further reform and economic support*
    b. *A limited number of professional guards were available, backed by relatively untrained (unpaid) trainees*
    c. *Continuing international support was needed*

5. *Central Asia:* OSCE was just getting involved, joint training programmes, the aim was to increase international aid in the area

Ambassador Zannier also highlighted the ongoing corruption in the countries occupying the "former soviet space", which would be heightened if border guards were poorly paid. Criminal groups were not slow to exploit such opportunities. The Ambassador also noted that the creation of borders had created social problems in many areas, a huge effort of cooperation and support was needed from the international community.

Havlicek took from the Ambassador's remarks that cooperation was the key, but she had seen that cooperation sometimes implied "a military risk". Giving the example of the Balkans, she argued that a political pre-requisite had to be built. But she returned to her earlier point that many parts of the world did not have the opportunities to implement EU norms and standards (lack of capacity) but which might hold the greatest risks.

Tlegen Suntayv, Deputy Chairman of the Customs Control Committee, Ministry of Finance of Kazakhstan, described the objective of facilitating the passage and flow of goods across the China–Kazakhstan border. Suntayv also stressed the need for a

cooperative operation. In essence this would be a "one stop operation" with one entry point.

Acknowledging that the international community had praised his committee's work, Suntayv described pilot studies and the ongoing work with neighbouring states. In agreement with Verrue, he argued that there was a necessity for customs staff to fight not only terrorism but also people- and drugs-trafficking.

PROBLEMS

Looking at the past, Suntayv repeated that agencies had to be coordinated. In his opinion, if collaboration had existed in the past, there would be fewer problems today. Ending on a positive note, he said Kazakhstan had attended the first ad-hoc meeting of the UN Security Committee – terrorism was seen to be a much greater threat – and had joined all 12 of the coordination committees.

Vyacheslav Kasimov, Director of the Executive Committee, Regional Anti-Terrorist Structure, Shanghai Cooperation Organisation (SCO), wound up the morning panel by describing the SCO's anti-terrorism activities. Introducing the topic, Kasimov described the instability of the SCO's region, where the activities of the Taliban and Al Qaida assisted various Islamic groups.

On the subject of internal issues, Kasimov argued that poverty, unemployment and a lack of food were underlying problems and that "corruption acts as fertile ground for terrorism". Acknowledging the insufficiently-protected borders, Kasimov said this meant that terrorists could be easily trained and move without problems. They were formed in rigid organisational structures and had efficient methods of exchanging intelligence and counter-intelligence.

After reviewing his role on the Executive Committee, Kasimov warned against duplication with other anti-terrorist structures. He explained that cooperation with the CIS states was excellent. Kasimov argued that conflict prevention was the main aim, and called for a framework to be created to fight separatism, terrorism and radicalism.

Examples of current activities of the SCO included:

- Actively working against the recruitment of terrorists
- Combating the terrorists' communication systems
- Fighting the illegal trafficking of WMDs that may be used by Islamic terrorists
- Undertaking joint training programmes
- Providing information on terrorists to international organisations

- Publishing quarterly bulletins on trends and steps taken
- Examining the roots and causes of terrorism to avoid future attacks

Kasimov concluded with a call to stop flows of drugs across the borders, as the ultimate destination was Europe. Havlicek thanked him warmly for his words and welcomed his call for multinational and regional groups to work together.

QUESTIONS AND ANSWERS

The Nonviolent Peaceforce's **Ben Reichert** wanted to know why the Georgia mission had been terminated. What were the likely next steps?

Ambassador Lamberto Zannier said that the problem was the need for inclusiveness, with Russia objecting to the operations. There were several options, hopefully involving Russia's involvement. However, another option would be bilateral assistance to Georgia.

Sasha Havlicek summed up the session and concluded that:

- There was a need for the US and the EU to further engage with Russia
- Cooperation between the US and the EU was ongoing but further global collaboration was needed
- New techniques and tools could be introduced but the impact on the trade capacity gap had to be watched carefully
- An international perspective was required in parallel with increased cooperation between border regional communities

Her final words, with which no one could disagree with, were "an enormous amount of work is still to be done".

BREAK-OUT GROUPS

BREAK-OUT GROUP A: HEALTH SECURITY AND NBCR THREATS

Overview: **Ian Abbott,** Chief of Policy and Planning Division, European Union Military Staff, chaired this break-out group and announced four main conclusions:

- There was a need to *improve communications with the public*, in a balanced way that combined information about risks and threats with education and heightened awareness
- *Work was required on detection systems*, and these needed to be targeted against genuine threats, i.e. what were we facing?
- There needed to be *much more coherence in stock-piling*, as there were major differences between the manner in which different nations (in Europe and internationally) approached the subject
- *Crisis management exercises were vital* – to educate the public and to increase awareness

Abbott described the approach taken, which had been to identify problems in four areas: threats, policies, capabilities and public confidence.

THREATS

The group was mainly concerned about the collection and coordination of intelligence information (this was flagged by the group as "red for danger"). Using the current communication methods, the public could be led to believe that everything was a threat and everyone was vulnerable. Abbott noted that as this was not feasible, priorities had to be identified.

POLICIES

The coherence and effectiveness of policies in the "C" and "B" sections of the NCBR threats were flagged as a matter of concern (red for danger). Public information on the threats was rated as between "very poor and non-existent". Worryingly, Abbott concluded that many nations appeared to hold a different perception as to whether there was a need to engage with the public.

CAPABILITIES

The break-out group felt that the emergency services could easily be swamped (red for danger) and that exercises would be a key way of reinforcing any message. On the matter of detection systems, a broad-based approach (using the assistance of other nations) was required. As medical care was now seen as a business, there was a major concern about the actual capacity available.

PUBLIC CONFIDENCE

The public information system was not rated highly while there was no confidence in any of the following: mutual support (nationally and internationally), confidence management itself and business continuity planning.

BREAK-OUT GROUP B: FREEDOM AND SECURITY

Overview: **John Richardson,** Chief Executive, European Foundation Centre, moderated a session with "Sold Out" signs on the door. Richardson observed that the break-out group continued with the theme of Javier Solana's keynote speech, i.e. *without trust and information sharing, we were lost.*

Richardson shared the break-out group's conclusions with the main meeting, and hit home with several points:

- There was a need to move from international norms and standards to international laws, particularly in regard to preventative detention
- No country could be an exception, e.g. the US had currently lost the opportunity to take the moral high ground
- Technology could protect citizens and also expose them
- A comprehensive and integrated strategy was required, one that combined human intelligence and technology
- There was a need to both stop terrorists and stop them being replaced
- In that sense, it had to be remembered that the people funding terrorists were "swimming in a sea of despair"

James Steinberg, Vice President and Director, Foreign Policy Studies, the Brookings Institution, wanted a balance between freedom and security. He suggested "high pay-off, low intrusion" systems. As the debate widened, Steinberg argued that the role of international organisations (outside of the US) was too important - they had to be involved in information sharing. As for actions to be taken, he wanted an international strategy that isolated and marginalised the sources of terrorism.

Stefaan Verhulst, Chief of Research, Markle Foundation, wanted a more public debate on the options available in the search for "freedom and security". On the subject of the use of technology, Verhulst said that intelligence gathering and a subsequent threat to use force may not deter terrorists, but it may deter those who harbour terrorists.

In conclusion, Richardson said that civil societies must work to expand freedom – it was "our greatest asset and our most powerful weapon".

BREAK-OUT GROUP C: WEB INDUSTRIES AND CYBER-SECURITY

Overview: **Boaz Gelbord**, Senior Security Expert, TNO Information and Communication Technology was in the chair for the third workshop. Like Richardson, Gelbord remarked in the lead-in to his conclusions on cyber-security, that technology could both protect citizens and expose them. One conclusion was that web security had become a vital factor in recent years as it was now seen to be part of the critical infrastructure. However, there was a lack of consensus permeating the workshop. Questions raised, but not answered, included:

- What was web security? (was it a denial of service or the fight against illegal music downloads?)
- Was protection of web content vital?
- Was censorship a major issue?
- Was product marketing (spam) a problem of the same magnitude?

Another issue raised was the fundamental way in which technology was changing. Technologies were converging rapidly and this was leading to regulatory and legal challenges. One thing was certain – technology was way ahead of the law enforcement and regulatory authorities.

The workshop was supported by a presentation by R. Fenton-May, Chairman, Carrierweb – a real-life example of tracking trucks by the use of GPS and GPRS systems. The presentation itself brought another factor into the mix, the information was extremely useful to the end-users (the customers; the SMEs who ran the trucking fleets)

but security issues were raised due to the vast amount of information available on the networks. The customers were the least concerned about security, it was left to the ISPs and the governments.

Gelbord concluded that in order to develop a consensus on these issues, there needed to be a clear definition of objectives and a constructive dialogue between all the players in order to produce a secure Internet environment and secure networks in general.

POLITICS, STRATEGY AND THE ROAD AHEAD

Former President of Finland and Co-Chairman of the Board of Directors of the EastWest Institute **Martti Ahtisaari** chaired the final panel. After hearing the reports from the workshops, he introduced **Ana Palacio**, Chairwoman, Joint Committee of the two Houses for European Affairs at the Spanish Parliament.

Palacio initially looked back to the days of the Cold War, when everything seemed straightforward in security terms. There were clear lines drawn, frontiers appeared to be sealed and the picture was asymmetric. Now, everything was different. Palacio referred to "porous" borders and saw a need for institutions to adapt to the new situation. She gave NATO as an example of an organisation that was doing just that. Threats were now asymmetric, it was hard to see where these threats were originating and the terrorists had no rules of engagement.

Moving on the US and the EU, Palacio argued they had different perceptions of the threat. While the US saw it as an "all out war", Europe was more concerned that they fought the battle with the "criminal code in one hand and the torch of freedom in the other".

WHAT WAS TO BE DONE?

Palacio identified the "name of the game", it was cooperation; meaning, "trust, awareness and understanding". Identifying three areas of action, Palacio moved towards the end of her remarks:

1. *Joint planning had to be deepened*: domestic tools had to be modernised, the June 2004 Action Plan was a step in the right direction, and the new Constitution could prove to be a catalyst for joint action in the future
2. *Future combined actions*:
   - What? - the answer: assistance in the case of attacks and reconstruction if an attack had taken place
   - Who? – the answer: use existing resources, especially NATO ("undergoing a fantastic process of adaptation"), use the "do-tanks" like the EWI and other societal networks
   - How? – the answer: develop shared interests, take concrete actions – "less talk"; present a united image
3. *Tackling the underlying causes*: there had to be a concerted effort to understand what motivated the terrorists; an "extremely difficult process", which examined factors such as education, politics, curbing radicalism, fighting poverty, etc.

After calling for more coordination of the US and EU strategies in the Middle East, Iraq and North Africa, Palacio called for "multi-facetted coordination against terrorism". She concluded that "they knew our vulnerabilities better than we understood the challenge ahead". Palacio argued that we had the tools, but we needed the political will.

George Russell, Co-Chairman of the Board of Directors of the EastWest Institute, was one of the final speakers. Russell focused on the growing participation of the private sector in the fight against terrorism. He had seen many examples of business involvement within the conference and he brought them together to illustrate his point:

- There had been a focus on the risk in the transport sector and the solutions were coming from the private sector; although more government–business coordination was required
- Microsoft (via Charney's presentation) were seen to be spending huge amounts to reduce the risk of cyber-terrorism
- Although not discussed at the conference, Russell gave the example of the NTI (Nuclear Threat Initiative) which was privately funded in order to keep WMDs out of terrorists' reach
- Chandler's "frightening exposé" of risk had come from the private sector
- GE's presentations' had shown that they were heavily involved in R&D work to identify and remove risks

Commenting on Faull's remarks, Russell acknowledged that private sector-government coordination was better in the US than in Europe. He noted that more entrepreneurial efforts were required in the latter and concluded by echoing Eckert's words – "governments and business must work harder and closer".

Vasil Hudak, Vice President, EastWest Institute, was the final speaker of the conference. Hudak looked at how the conference had met its objectives and possible next steps.

He was pleased that the conference had broadened the debate away from the US and the EU, by including speakers from (and a debate on) Central Asia, Russia and the Caucasian republics. Hudak had welcomed the "sense of reality" that had been brought to Brussels. A cross-organisational approach had been suggested by the EWI and several speakers had taken up the call. The focus on technology had been

welcome but Hudak noted that there was still much work to be done. He had two essential messages from the conference:

- The threat was "asymmetric and network-based" and needed an "asymmetric, network-based response"; it had to be flexible, rapid, broad-based and global
- The response had to be based on international partnerships of governments, businesses and civic associations

Quoting Javier Solana, Hudak said, "because terrorism is a global phenomenon, we need a global response". This led him to the next steps that the EWI would be taking:

1. selecting three to four areas of in-depth focus for 2005
2. creating international & cross-sectoral Expert Groups
3. presenting regular fora in Brussels and beyond (further East)
4. planning the 3rd Worldwide Security Conference (2006)

After thanking everyone involved in the conference organisation, **Martti Ahtisaari** closed the conference by declaring that it had been a good example of cooperation, especially from the private sector. However, he noted that everyone present had a responsibility to understand what was happening and to be part of the response against the current threats.

The EWI thanks all speakers, participants and sponsors for contributing to the success of the Second Annual Worldwide Security Conference. The Global Security Program is committed to fostering this dialogue and we are looking forward to cooperating with you in future.

For more information please visit our
website www.ewi.info or contact us at brussels@ewi.info.

EDITORIAL TEAM

Communications Manager	Rebecca Weaver
Editors	Erol Spencer Hofmans
	Christine Weyrich
Reporter	John Chapman
Graphics	Vítek Šmejkal
Photographer	David Plas

The website of the conference is available at http://wsc.ewi.info .

EastWest Institute

Bridging Divides

Special Thanks to:

Microsoft

WORLD CUSTOMS ORGANIZATION
ORGANISATION MONDIALE DES DOUANES

CARRIERWEB

EASTWEST INSTITUTE

Bridging Divides

« Ladies and gentlemen, dear friends, the fight against international terrorism is a clear priority for the EU. For this global threat we need a comprehensive strategy. We must combine measures to stop specific individuals or networks with long-term measures to stabilise and transform societies. And exactly like your conference does, we need to bring together people from a wide variety of backgrounds and nationalities. »

Javier Solana, EU High Representative of the Common Foreign Security Policy
Second Annual Worldwide Security Conference





"…As a European-American "think and do tank", EWI is committed to strengthening international security and addressing critical challenges of the 21st century. …We have to rethink how we approach borders to protect states and citizens against threats while improving the flow of goods and people."

John E. Mroz, President and CEO of the EastWest Institute
Second Annual Worldwide Security Conference