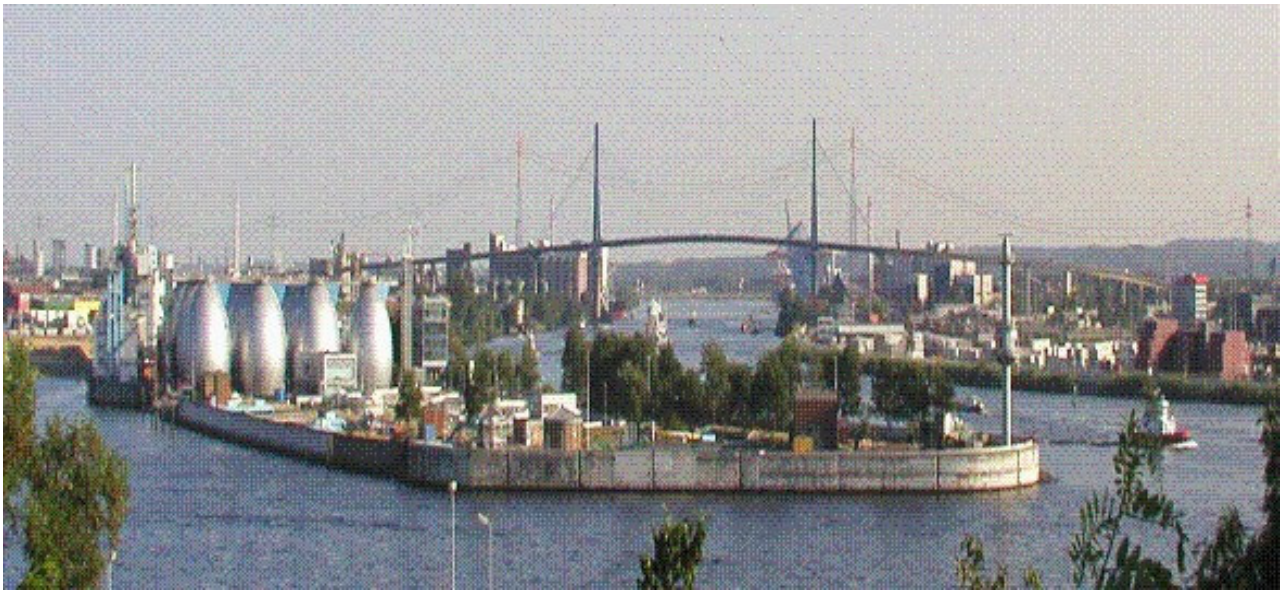
SECURITY &
DEFENCE AGENDA

SDA
SECURITY & DEFENCE AGENDA

Defending Europe's Vulnerable Infrastructure



SDA Roundtable

2 October 2006, Brussels
Rapporteur: John Chapman

Organised with the support of HP

CONTENTS:

PROGRAMME OF THE DAY p. 3

EXECUTIVE SUMMARY p. 4

DEBATE HIGHLIGHTS p. 5

SESSION 1 – ARE EU GOVERNMENTS COLLABORATING ON INFRASTRUCTURE PROTECTION? p.6

PANELLISTS
JOSÉ ANTONIO HOYOS PÉREZ
TIJEN KHOEN LIEM
ERIC LUIIJF

SESSION 1 – Q&A p. 9

SESSION 2 – ARE THE EU'S WEAKEST POINTS INSIDE OR OUTSIDE EUROPE? p. 11

KEYNOTE SPEECH – ANATOLY SAFONOV p. 11

PANELLISTS
ANATOLY SAFONOV
LINDSAY CLUTTERBUCK
MIODRAG PESUT
JOHN P. SMITH

SESSION 2 – Q&A p. 14

LIST OF PARTICIPANTS p. 17

ABOUT THE SDA p. 22

PROGRAMME OF THE DAY

SDA Monthly Roundtable, Bibliothèque Solvay, October 2, 2006, 12:00-16:00

Defending Europe's vulnerable infrastructure

ARE EU GOVERNMENTS YET COLLABORATING ON INFRASTRUCTURE PROTECTION?

Session I 12:00-13:30

Within ten days of the SDA's mid-2005 roundtable on critical infrastructure protection, London's transport system was hit by four near-simultaneous bomb attacks. This underlines yet again that if anti-terrorism protection and emergency response is fundamentally local, intelligence gathering and sharing must be international. Are we any closer to coordinating policies at an EU level to prevent critical infrastructure failures? Is a net centric approach to critical infrastructure protection viable? Is there a sufficient level of private sector involvement in the development of preparedness strategies? What roles can the EU and NATO play in coordinating international efforts?

Moderator; **Giles Merritt**, Director, Security & Defence Agenda

- **José Antonio Hoyos Pérez**, Policy Officer, Protection of energy facilities and critical infrastructure, European Commission: DG Energy and Transport
- **Tjien Khoen Liem**, Policy Officer, Preparatory Action for Security Research, European Commission: DG Enterprise and Industry
- **Eric Luiijf**, Principal Consultant for Critical Infrastructure Protection & Info Ops, Clingendael Centre for Strategic Studies (CCSS)/TNO Defence, Security & Safety

SDA Members' Lunch:
13:30-14:30

ARE THE EU'S WEAKEST POINTS INSIDE OR OUTSIDE EUROPE?

Session II 14:30-16:00

Europe's dependence on imported energy means that its infrastructure protection strategies now extend as far east as Central Asia, if not worldwide. What defensive strategies should EU policymakers be considering? What different levels of priority should they be giving to the strengthening of purely domestic infrastructures like transportation and power generation while also considering infrastructures that transcend national boundaries, such as the internet?

Keynote Speech by ANATOLY SAFONOV, Special Representative of the Russian President on international cooperation in the fight against terrorism and transnational organised crime

Moderator: **Giles Merritt**, Director, Security & Defence Agenda

- **Lindsay Clutterbuck**, Research Leader, Defence & Security, RAND Europe
- **Miodrag Pesut**, Officer, Transport and Infrastructure Development Section, United Nations Economic Commission for Europe (UNECE)
- **John P. Smith**, Manager of Strategy and Planning, Hewlett-Packard

EXECUTIVE SUMMARY

The European Commission has been active since the SDA's last debate on critical infrastructure protection in 2005. Following an extensive consultation process, it has issued a comprehensive Green Paper, emphasising public-private cooperation and the protection of all sectors against all hazards. Unfortunately, hardly any of the agreements likely to result from the consultation have been made public.

One problem is the timing, with the Commission's Policy Package not due until November, while another is the need to discuss matters "behind closed doors". The Commission's **Tjien Khoen Liem**, Policy Officer for Preparatory Action for Security Research, stated that cooperation had to go beyond the exchange of best practices and all speakers supported that view.

The Clingendael/TNO Centre for Strategic Studies' **Eric Luiijf** listed examples of the lack of international cooperation, especially between the public and private sectors. He asked some key questions – what is really 'critical' and who is responsible for the all hazards protection of critical infrastructure? The funding questions can only be answered after clear answers to these questions have been given.

Giving a keynote address, President Putin's Special Representative for international cooperation in the fight against terrorism and transnational organised crime, **Anatoly Safonov**, outlined the global dimension that Russia was bringing to the security dialogue as part of its G8 Presidency. Russia was willing to contribute fully, via both bilateral agreements and with bodies such as the EU. In total agreement, UNECE's **Miodrag Pesut** called for a global cross-sector approach that brought together all of the major players.

Several speakers wanted an increased focus on the protection of information systems, a critical part of all essential industries. In that regard, perhaps the most telling point came from HP's **John P. Smith**, who referred to US government projects that had an average time span of 11 years, while his organisation aimed to produce new products every 9-18 months. That gap would be extremely hard to bridge.

DEBATE HIGHLIGHTS

RECOMMENDATIONS FOR THE FUTURE

- International cooperation in the area of critical infrastructure protection should go beyond the exchange of best practices.
- A global, cross-sector approach will aid the process.
- Public-private partnerships in this area are essential - as is understanding the different roles and tasks involved in these partnerships.
- A multilateral producer-consumer dialogue between all relevant stakeholders would be useful especially in the energy sector.
- Efforts to synchronise government and private sector project cycles could help increase the effectiveness of private-public cooperation.

SESSION I HIGHLIGHTS

- The EU wants to coordinate the activities of its Member States and assure the public that necessary terrorist alert programmes are in place.
- Following the launch of the Commission's Policy Package on CIP in November 2006, there will be a need to explore the potential for close cooperation with the EU's neighbours – including Russia, Algeria & Norway, due to the importance of energy networks – and with third countries in general.
- Looking at the full incident cycle of a disruption can provide keys to an all-hazards approach to CIP: this implies increasing redundancy within infrastructure, i.e., by removing single points of failure within a complete network or chain of critical processes.
- Funding opportunities within DG Justice, Freedom and Security include €3.7 million to date, €4.5 million in the offering and a further €12.4 million foreseen for 2007.
- EU borders are some of the world's best protected, yet major terrorist incidents had originated within national boundaries.

SESSION 2 HIGHLIGHTS

- A Global Forum of Antiterrorist State and Business Partnership will be convened in Moscow on 28-30 November 2006. The outcome of the forum will be a draft strategy, including recommendations for the protection of critical infrastructure.
- Consequences of attacks on both critical national information infrastructure (CNII) as well as on critical national infrastructure, could be regional, national or global – the only way to combat such threats is via effective public-private cooperation.
- The Energy Security Forum, a body formed under the auspices of UNECE, aims to reconcile the viewpoints of the energy industry, financial institutions and governments. A recent forum study concluded that security risks had increased sharply due to a rising demand for oil in developing countries, the rise in – and volatility of – oil prices and the restricted access for energy companies to hydrocarbon reserves in some countries.
- Commercial considerations have driven some companies to simplify networks, making them more vulnerable.

SESSION 1: ARE EU GOVERNMENTS COLLABORATING SUFFICIENTLY ON INFRASTRUCTURE PROTECTION?

The question on the table was whether EU Member States and the European Institutions were cooperating satisfactorily. This meant in terms of sharing intelligence, strategies, in building bridges between the public and private services, and in utilising the potential benefits of bodies such as the EU and NATO.

THE COMMISSION'S PERSPECTIVE

José Antonio Hoyos Pérez, Policy Officer for the Protection of energy facilities and critical infrastructure in DG Energy and Transport

José Antonio Hoyos Pérez, DG Energy and Transport

Policy Officer **José Antonio Hoyos Pérez** described the work completed by the Commission since the "Communication on critical infrastructure protection in the fight against terrorism" of October 2004. The first result had been 2005's Green Paper, which will be furthered by proposals of the Commission to be adopted before in 2006. The Commission's objective is to launch a European Programme for Critical Infrastructure Protection, which will set the framework for general application but will need to be developed at the sectoral level. In particular, a Communication on Energy and Transport Critical Infrastructure is also under preparation in this context. According to Hoyos Pérez, on top of the direct damage to people and to assets, the potential for serious economic disruption if energy or transport European infrastructure is severed, had been a main driver for taking a European initiative.

The Commission's Green Paper on Critical Infrastructure Protection

- responds to the Council's request to create a "European Programme for Critical Infrastructure Protection" (EPCIP).
- addresses such key issues as:
  - What should EPCIP protect against?
  - Key principles
  - The type of framework needed
  - Definition of EU Critical Infrastructure
  - National Critical Infrastructure
  - Role of Critical Infrastructure owners/operators
  - The Critical Infrastructure Warning Information Network (CIWIN)
  - Funding
  - Evaluation and monitoring

Tjien Khoen Liem, Policy Officer for Preparatory Action for Security Research in DG Enterprise and Industry

Policy Officer **Tjien Khoen Liem** complemented Pérez's contribution. He focused on the security research programme, now part of the Seventh Framework Programme (FP7). Acknowledging the international dimension of terrorism, he stressed that the EU wanted to coordinate the activities of the Member States and assure the public that necessary terrorist alert programmes were in place.

Describing ongoing actions, Liem listed the objectives agreed at a recent informal meeting between EU Ministers and Commissioner Frattini. These included:

- The reduction of radicalisation and recruitment of potential terrorists
- Making the Web less useful to terrorists


Tjien Khoen Liem, DG Enterprise and Industry

- Research into liquid explosives
- Ensuring that risk and impact assessments are central themes
- Sharing expertise between member states

Liem also declared the importance of building security into new products and materials, so that they were less useful to terrorists. As examples, he suggested that in the future, it could be feasible to negate the risks of aircraft being flown into buildings and to make fertiliser less suitable for terrorist purposes.

> "Do we need more coordination between EU member states? That is a life and death question."
> Tjien Khoen Liem

However, Liem added that technology alone would not win the day, as it was essential to address social problems. Describing the "toolbox" approach to security research, Liem described the various sizes of projects that had been suggested by the European Security Research Advisory Board (ESRAB). The draft Security Research programme would include one "demonstration" project (€ 30-40 million) in the mass transportation sector, preceded by a pilot project (€ 2-5 million).

In conclusion, Liem asked if the current plans showed sufficient coordination between Member States and the institutions, and whether there was a need for more community funding. In any event, he was sure that co-operation had to go beyond an exchange of best practices.

Security research priorities

- Security for citizens
- Intelligence surveillance
- Border security
- Restoring services following a crisis

In the follow-up Q&A sessions, **Magnus Ovilius,** Head of Sector Preparedness and Crisis Management in DG Justice, Freedom and Security, reiterated that the consultation process had involved an extensive public-private dialogue and that an "all-hazards approach" was the order of the day (threats to information systems, cyber crime, denial of services, as well as protection of energy and transport networks). Following the launch of the Commission's Policy Package in November, Ovilius said there would be a need to explore the potential for close co-operation with the EU's neighbours – including Russia, Algeria and Norway, due to the importance of energy networks – and with third countries in general.

A CONSULTANT'S VIEW

Eric Luiijf, Principle Consultant for CIP & Info Operations at the Clingendael/TNO Centre for Strategic Studies


Eric Luiijf, the Clingendael/TNO Centre for Strategic Studies

After commenting on the EU's definition of CIP, **Eric Luiijf,** Principle Consultant for CIP & Info Operations at the Clingendael/TNO Centre for Strategic Studies, wanted to know who was responsible for the protection of such critical infrastructure, especially as 80% of it was in the hands of the private sector. Luiijf described recent studies showing that while private enterprises were capable of protecting their own assets, they were sometimes aware of the upstream ramifications but certainly not about the downstream ramifications of critical infrastructure failure (all hazards).

> Protection measures are often different on each side of a border.
>
> Eric Luiijf

Looking at potential disruptions in energy supplies, telecommunication networks, water supplies, water level management, the possibilities of outbreaks of disease, etceteras, Luiijf made a case for looking at the full incident cycle, rather than just protection of a single asset. This implied increasing the redundancy within infrastructure, i.e. by removing single points of failure within a complete network or chain of critical processes.

In this domain, Luiijf argued that national and European emergency management systems were not always aware of critical infrastructures and the related inter-connections. In essence, there was a lack of public-private co-operation. Another weakness identified was in cross-border co-operation, where Luiijf stated that actions were often taken only on one side of the border. He had seen cases where both public and private emergency support could not cross borders for legal and other reasons. Luiijf wanted a possibility for EU laws to swing into action, ones that, in the case of emergencies, overrode national laws and EU regulations that were only developed for normal conditions.

SESSION I: Q&A

WHERE DOES COORDINATION BEGIN AND END?

SDA Director **Giles Merritt** had heard the Commission's overview of the situation, and he repeated Liem's earlier question – was more coordination needed between the Member States and the EU?

Miodrag Pesut, an Officer in the Transport and Infrastructure Development Section at the United Nations' Economic Commission for Europe, saw events from a global perspective. Players to-date included the G8 members, the UN, the EU and there had been a Ministerial Conference on International Transport Security in Tokyo in January 2006. He had seen many examples of co-operation in the last five years, and he felt that the basis of all responses should be at the national level.

Luigi Rebuffi, Thales

As for public-private cooperation, Thales' Director for European Affairs, **Luigi Rebuffi**, was concerned that infrastructure owners would not release information as they thought it would increase their vulnerability to attack. UK Delegation to NATO's Defence Counsellor, **Paul Flaherty** wanted to know how intelligence, information and knowledge could be shared in an EU context, and with other organisations. He also reasoned that, if 80% of CI was in private hands and essentially international in nature, any preparatory actions had to go far beyond the EU's boundaries.

Summing up the feeling of many, Luiijf said he wanted everyone – EU, nations, public and private enterprises - to get their ducks in a row. Some nations were not involved, some operators were not involved – this had to change.

FUNDING – COSTS AND BENEFITS

Merritt inquired if a set of dedicated budgets should be set aside, purely for the protection of the EU's citizens. Looking at the costs of terrorist attacks, post 9/11, Pesut described additional costs to the airline industry of $35 billion, together with significant ones for maritime transport. He therefore wanted to make cooperation between the public and private sectors more attractive for the latter.

Magnus Ovilius, DG Justice, Freedom and Security

Magnus Ovilius described funding opportunities within his DG, including €3.7 million to-date, €4.5 million in the offing and a further €12.4 million foreseen for 2007.

POST-INCIDENT PLANNING AND RESPONSE?

The chaos at Heathrow airport following the discovery of the plans for liquid bomb attacks had not impressed Merritt. He had not seen much application of best practices and Merritt wanted to know how such situations could be improved.

Ovilius did not agree. He had seen good co-operation between the Civil Aviation Authorities and the EU intelligence services on the new civil aviation security measures to be adopted as a response to the new terrorism threat involving the use of liquid explosives..

The actions taken had been just about right ("not too stringent, not too soft").

Merritt understood that cooperation may have looked good from the inside, but it had appeared to be confusing to the public. There had been long queues, severe disruption, rules for hand-baggage introduced and then repealed. He wanted more communication of foiled attempts, better public relations with partners and greater inter-action with the public. Such publicity could deter future terrorist attacks.

TRANSPORT OR ALL SECTORS?

Merritt commented that all of the major terrorist attacks to-date had been on transport infrastructure, and asked if that should be the priority with special actions being necessary. Pesut reasoned that while the transport infrastructure was the most vulnerable, it was almost impossible to protect, as it was "an open system" with 5,000 kilometres of track.

Flaherty wanted more attention paid to information networks, as they were a critical part of all physical assets. Perez and Liem supported this view, with the latter arguing that society was now dependent on the Internet. Luiijf was of the same opinion, listing several incidents where IT systems – and especially process control systems/SCADA in critical infrastructures - had been vulnerable.

CROSS-BORDER CO-OPERATION

Pesut did not agree with Luiijf's earlier assertion that cross-border co-operation was a problem, as EU borders were some of the world's best protected. In addition, the major terrorist incidents had originated within national boundaries, rather than being external in nature. Luiijf responded that his view stems from an all hazards – not terrorists only approach to critical infrastructure. If incidents did affect more than one country, the EU PASR project VITA (Vital Infrastructure Threats and Analysis), for example, showed that there was a great risk that response systems would often be limited to one side of the border only.

KEYNOTE SPEECH: ANATOLY SAFONOV

Special Representative of the Russian President on the issue of international cooperation in the fight against terrorism and trans-national organised crime

Anatoly Safonov, Cabinet of the Russian President

Opening his remarks, Anatoly Safonov stressed the importance of protecting critical infrastructure, and emphasised the significance of global energy supplies. This subject was one of the main priorities of Russia's G8 Presidency.

Focusing on energy, Safonov reminded the audience that terrorist attacks could cause widespread disruption even when conducted with a minimum set of weapons. These consequences could be as great as those conducted with WMDs. Safonov's solution was to be proactive, as any attempt to build protective walls around a nation would soon turn it into a prison.

> If we attempt to hide within a fortress, it will soon become a prison.
>
> Anatoly Safonov

These proactive measures had to involve the private sector, as the majority of the critical infrastructure was in its hands. Russia had been successful in developing a real public-private partnership, and Safonov was confident that a similar approach would be successful in the international arena. That was the reason for Russia's initiative along these lines, recently launched under the auspices of the G8 and welcomed by all participants.

Russia's key principles

- Developing mutual interests and co-operation based on good will and equality
- Understanding the different roles and tasks of a public-private partnership in terms of counteracting terrorism

Russia's aim was to develop specific practical projects (based on state-business co-operation) that would take full consideration of economic factors and interests. Workshops were being held and a Global Forum of Antiterrorist State and Business Partnership will be convened in Moscow on 28-30 November 2006. The outcome of that forum would be a draft strategy, which would include recommendations for the protection of critical infrastructure - developed on the assumption that there were long-term global threats. Safonov insisted that Russia wanted global participation and that his nation was ready to make a full contribution.

Expert Workshop – October 2006 (Moscow)

- national agencies and representatives of Russian and foreign companies
- to discuss projects and exchange best practices
- with a particular focus on the funding of terrorism:
  - preventing illegal funds being used
  - facilitating a global system to counteract such funding
- over 20 projects presented (e.g. by Gazprom, Finmeccanica, General Electric, etc.)

SESSION 2: ARE THE EU'S WEAKEST POINTS INSIDE OR OUTSIDE OF EUROPE?

AN INDEPENDENT THINK-TANK'S VIEW

RAND Europe's **Lindsay Clutterbuck**, Defence & Security Research Leader, focused on the Internet, a vital component of the Critical National Information Infrastructure (CNII), itself part of the Critical National Infrastructure (CNI).

Lindsay Clutterbuck, RAND Europe

While Clutterbuck could see the Internet's benefits, in its support of the CNI, he wanted to focus as well on the problems caused by the potential for exploitation by terrorists. Consequences of attacks on both the CNI and the CNII could be regional, national or global. The only way to combat such threats was via effective public-private co-operation. Listing the ways in which terrorists used the Internet (recruitment, training, raising funds, potentially carrying out attacks, etc.), Clutterbuck stressed the need to stop it being used to encourage radicalization and ultimately, recruitment to the terrorist cause.

The Internet – dark / light side

- Global access to information, but with
- Global opportunities for those wishing to cause widespread disruption

> The relationship between Governments and the private sector should be based on cooperation not coercion and partnership not primacy.
>
> Lindsay Clutterbuck

ON BEHALF OF THE UNITED NATIONS

Miodrag Pesut, an Officer in the Transport and Infrastructure Development Section at the United Nations' Economic Commission for Europe, outlined the UN's work in developing a legal framework for combating terrorism and its achievement in defining a Global Counter-Terrorism Strategy[1] - established in September 2006.

Miodrag Pesut, United Nations' Economic Commission for Europe

The UNECE – one of five regional commissions – creates legal instruments and is steered by its member countries. To-date 55 international agreements and conventions have been finalised in the transport sector (e.g. dangerous goods, cross-border flows, etc.). In terms of security of infrastructure, UNECE is weighing up the interests of its member Governments to initiate, considering security aspects of infrastructure agreements, and is waiting for their guidance.

[1] See http://www.un.org/terrorism/strategy/ for full details of the Strategy.

Producer-consumer dialogue – focus areas

- data and information sharing and increased transparency
- infrastructure investment and financing
- legal, regulatory and policy framework
- harmonization of standards and practices
- research, development and deployment of new technologies
- investment / transit safeguards and burden sharing

Pesut moved on to the Energy Security Forum[2], a body formed under the auspices of the UNECE, which aimed to reconcile three viewpoints – those of the energy industry, financial institutions and governments. It had recently submitted its findings of a study on *Emerging Energy Security Risks and Risk Mitigation in a Global Context* to the Russian Government ahead of the G8 Summit. The Forum concluded that security risks had increased sharply due to a rising demand for oil in developing countries, the rise in - and volatility of - oil prices and the restricted access for energy companies to hydrocarbon reserves in some countries. It therefore recommended more investment in the energy sector in order to foster public-private partnerships. The first step would be a new multilateral producer-consumer dialogue between all relevant stakeholders (see table above).

> Some nations are not doing enough – we need to show them the way
>
> Miodrag Pesut

AN INDUSTRY VIEW ON THE INFORMATION SECTOR

John P. Smith, Manager of Strategy and Planning at Hewlett-Packard, compared the transport and the information systems networks. Both were open – in the sense that anyone could participate - and were therefore vulnerable. Smith likened a person travelling around the global transport network to a data packet on the information highway, both had freedom to roam but they had to be protected.

John P. Smith, Hewlett-Packard

Layered approaches were the answer, so that, ultimately, networks could be capable of healing themselves. Unfortunately, commercial considerations had driven companies to simplify networks and this had made them more vulnerable. Smith warned against assumptions when it came to the subject of security, mentioning that his company wanted to continue its participation in cooperative research. HP was already spending $2 billion per annum in various government partnerships, including work with the EU.

> The average cycle of US government projects takes 11 years, while HP produces products every 9 -18 months.
>
> John P. Smith

Smith concluded with a warning: it took the US government an average of 11 years to complete a project cycle, whereas HP produced new products every 9-18 months.

[2] The Energy Security Forum comprises members of the energy industries and financial sector under the auspices of the United Nations Economic Commission for Europe.

SESSION II: Q&A

USE OF THE INTERNET

Magnus Ovilius commented that the Commission was looking at ways of stopping radicalisation and recruitment of terrorists, criminalisation, advice on bomb-making, etc. via the Internet. However, he acknowledged that it could only impact activities originating within the EU.

THE IMPACT OF FURTHER EU ENLARGEMENT

Merritt asked if Russia and the EU were ready to talk about the shared problem of security in the Black Sea and Caucuses regions, following the arrival of Romania and Bulgaria within the Union. In response, Ovilius said that the representatives of the Member Sates (the Critical Infrastructure Protection (CIP) contact points) were talking to the operators (as part of the public-private dialogue) and that it was essential to develop consensus between all EU members (of the EU-27) before talking to third countries.

Compatible solutions had to be agreed across the EU. One problem outlined by Ovilius was that private enterprises (such as banks) may be reluctant to share information related to weaknesses and vulnerabilities. The result was that sometimes such discussions had to be held "behind closed doors".

Luigi Rebuffi took the discussion further, suggesting it was necessary to go beyond the G8 - to China and India, as they would be major energy players in the future. Pesut saw the necessity to raise the capacity of partners so that everyone was on an equal footing and common issues could be discussed.

RUSSIA'S PREFERENCE – TO DEAL WITH INDIVIDUAL MEMBER STATES OR WITH THE EU?

Responding to Merritt's question, Safonov said Russia had adopted a multi-facetted approach (EU and bilateral agreements). This was proving successful with fruitful co-operation between Russia and agencies such as Europol and Eurojust. The fight against terrorism obviously went beyond the EU's borders and there was a need to look to the long-term – "to win the minds of future generations".

Safonov added that within the Permanent Mission to the EU, there were experts representing leading agencies within Russia. The need was to develop real-time co-operation with the EU as a whole. In addition, Russia's special services were becoming more open and were collaborating with, for example, the UN, the EU, NATO and the OSCE. Global co-operation was the name of the game. The energy sector dialogue launched at the G8 was not limited at all in its scope. Such approaches had to contain input from nation states, the business world and experts in relevant disciplines.

IS A SECTORIAL APPROACH THE RIGHT WAY?

Flaherty had heard views about a sectorial approach, and given that this implied the existence of a single model, he asked if the EU was prepared to go that way. Luiijf understood the merits of such an approach but he felt this would lead to some "quick wins" being missed, as they were cross-sectorial. Pesut added that if sectors varied in their vulnerability, different technical approaches might be necessary. Whatever approach was taken, Smith emphasised the need for total trust between partners.

Merritt concluded that it was not communication across borders that was the most important factor, but communication itself. All partners had to be involved, and have access to all the information necessary to be able to adapt to meet common problems.


Participants at Bibliothèque Solvay.


Magnus Ovilius and Tjien Khoen Liem


Giles Merritt moderating the first session


H.E.. Štefan Füle, Czech Ambassador to NATO


The Panel in the second session


Hanif Ahmadzai, Mission of Afghanistan to the EU

LIST OF PARTICIPANTS 2 OCTOBER 2006

Patrick Ahern
Policy Advisor, *European Organisation for Forwarding, Transport, Logistics & Customs (CLECAT)*

Hanif Ahmadzai
Second Secretary, *Mission of Afghanistan to the EU*

Muzaffer Akyildirim
Counsellor on Defence, *Mission of Turkey to the EU*

Jan Alhadeff
Administrator, Capabililities, Armaments, Terrorism/ESDP, Space Matters & EU/NATO Relations, *Council of the European Union: Directorate General for External and Politico-Military Affairs*

Jane Alkhouri
Mission of Canada to the EU

Vladimir Andreev
Deputy Director, Department of New Challenges and Threats, *Ministry of Foreign Affairs, Russia*

Laura Antonelli
Attache d'Ambassade, *Mission of Switzerland to the EU*

Pierre Apraxine
Deputy Chief of Delegation, *International Committee of the Red Cross (ICRC) EU Liaison Office*

Andrey Avetisyan
Minister Counsellor & Deputy Head of Mission, *Mission of the Russian Federation to the EU*

Michele Barsanti
General Electric International (GE)

Stephen Blake
Consultant, *Kroll London*

Catherine Boucher
First Secretary, Security and Defence, *Mission of Canada to the EU*

Paulo Brito
Assistant Secretary to the Defence Committee, *Assembly of the Western European Union*

Edgar Buckley
Senior Vice President, Marketing, *Thales*

Adam Bugajski
Second Secretary, *Delegation of Poland to NATO*

Andreea Bulgaru
Personal Assistant to Economic Minister, *Embassy of Pakistan to Belgium*

Caroline Calvez
European Company for Strategic Intelligence

Geert Cami
Managing Director, *Security & Defence Agenda*

Carlo Cerrina
Assistant Defence Advisor, *Delegation of Italy to NATO*

John Chapman
Rapporteur, *Security & Defence Agenda*

Vladimir Chizhov
Ambassador, *Mission of the Russian Federation to the EU*

Lindsay Clutterbuck
Research Leader, Defence & Security, *Rand Europe - Cambridge*

Gaïd-Marie Cocher
Data Analysis and Policy Studies Manager, *AeroSpace and Defence Industries Association of Europe (ASD)*

Daniela Coleman
Policy Officer for the Security and Defence Committee, *American Chamber of Commerce to the EU (AmCham EU)*

Kathleen Conway
Attache, US Customs and Border Protection, *Mission of the United States of America to the EU*

Robert Cox
Trustee, *Friends of Europe*

Marzio Cuoco
National Armaments Director Representative, *Permanent Representation of Italy to the EU*

Alessandro D'Andrea
Naval Assistant Armaments Attaché, *Delegation of Italy to NATO*

Robin Davies
Defence Attaché, *Embassy of the United Kingdom to the Netherlands*

Ludwig Decamps
Policy Planning Advisor, *North Atlantic Treaty Organisation (NATO)*

Elina Eloranta
Visiting Researcher, *Université Libre de Bruxelles (ULB)*

Indulis Emsis
Chairman, *Latvian National Parliament, National Security Committee*

Nicholas Fiorenza
NATO and EU Affairs Correspondent, *Jane's Defence Weekly*

Paul Flaherty
Defence Counsellor, *Delegation of the United Kingdom to NATO*

Jan Foghelin
Head of Division, Defence Analysis, *Swedish Defence Research Agency (FOI)*

Štefan Füle
Ambassador, *Delegation of the Czech Republic to NATO*

Gerard Galler
Official, Internet, Network & Information Society, *European Commission: Directorate General for Information Society & Media*

Bill Giles
Director General Europe, *BAE Systems*

Annette Godart van der Kroon
President, *Ludwig Von Mises Institute Europe*

Sara Goldberger
PR & Communications Manager, *AeroSpace and Defence Industries Association of Europe (ASD)*

Fernando Gomez Ochoa
Senior Police Officer, Chief of Security Department, *Spanish National Police*

Grégory Gosp
European Affairs Manager, *Thales*

Douglas Gregory
Vice-President Governmental Programs EMEA, *IBM Belgium*

Michael Grimes
Consultant, *Security & Defence Agenda*

Rainer Hellmann
Journalist, *Fuchsbriefe*

Jean Claude Hemmerechts
Public Safety/Homeland Security - Public Sector Europe, *Cisco Systems Belgium*

Jessica Henderson
Project Manager, *Security & Defence Agenda*

Arnauld Hibon
Vice-President, Director EU Affairs, *Eurocopter*

Jose Antonio Hoyos Perez
Policy Officer, Protection of Energy Facilities and Critical Infrastructures, *European Commission Directorate General for Energy & Transport*

Arnaud Jacomet
Head of Secretariat General, *Western European Union (WEU)*

Bozena Jekot
First Counsellor, JHA, *Permanent Representation of Poland to the EU*

Gareth Jones
Coordination Manager - NATO, EU and Cooperation, *Thales*

Miroslav Jovanovic
Defence Attaché, *Embassy of the Republic of Serbia to Belgium*

Linda Karvinen
Senior Manager, *Security & Defence Agenda*

Takekazu Kawamura
Ambassador, *Mission of Japan to the EU*

Marika Konings
Director European Affairs, *Cyber Security Industries Alliance*

Leo Koolen
Policy Developer, Internet, Network and Information Security, *European Commission: Directorate General for Information Society & Media*

Girts Valdis Kristovskis
Vice-Chairman, *European Parliament: Subcommittee on Security and Defence (Committee on Foreign Affairs)*

Brice Lançon
Director, European Affairs, *Safran Group*

Peter Lennon

Tjien-Khoen Liem
Policy Officer, Preparatory Action for Security Research, *European Commission: Directorate General for Enterprise and Industry*

Ahto Lobjakas
Journalist, *Radio Free Europe*

Eric Luiijf
Consultant for Critical Infrastructure Protection & Info Ops, *Clingendael Centre for Strategic Studies (CCSS)/TNO Defence, Security and Safety*

Michal Malovec
Administrator, *European Parliament*

Micol Martinelli
Adviser International Affairs, *Association of European Chambers of Commerce & Industry (EUROCHAMBRES)*

Guy Meguer
Solutions Marketing Director- Homeland Security, *European Aeronautic Defence and Space Company (EADS)*

Claudio Mereu
Partner Resident, *McKenna Long & Aldridge*

Vittorio Merola
Project Assistant, *Security & Defence Agenda*

Giles Merritt
Director, *Security & Defence Agenda*

Megan Minnion
Programme Coordinator and Information Officer (Finland, Ireland, Kazakhstan, Sweden, Tajikistan and Uzbekistan), *North Atlantic Treaty Organisation (NATO)*

Milena Mitic
First Secretary, Transatlantic Relations, *Mission of Serbia to the EU*

Richard Narich
Ministre Plénipotentiaire, Conseiller du Directeur, *Institut national des hautes études de sécurité (INHES)*

Egidijus Navikas
Counsellor, *Permanent Representation of Lithuania to the EU*

Lukasz Odelga
EU Policy Officer, *Regional Office of Silesia in Brussels*

Magnus Ovilius
Head of Sector, Preparedness and Crisis Management, *European Commission: Directorate General for Justice, Freedom and Security*

Pasi Pasivirta
Long Term Vision Co-ordinator, *European Defence Agency (EDA)*

Miodrag Pesut
Officer, Transport and Infrastructure Development Section, *United Nations Economic Commission for Europe (UNECE)*

André Pirlet
Project Manager "New Projects", *European Committee for Standardization (CEN)*

Nicolas Pomey
Consultant, *Avisa/JHL Conseil*

Tariq Iqbal Puri
Economic Minister, *Mission of Pakistan to the EU*

Gerrard Quille
Specialist Security and Defence, Policy Department, *European Parliament: Directorate General External Policies*

Luigi Rebuffi
Director for European Affairs, *Thales*

Piotr Rosolak
Colonel, Operations/Exercises Division, *European Union Military Staff*

Boris Rousseff
European Representative, *Canadian European Roundtable for Business (CERT)*

Anatoly Safonov
Special Representative of the President on the issue of international cooperation in the fight against terrorism, *Cabinet Office, Russia*

Paolo Salieri
Policy Officer, Preparatory Action for Security Research, *European Commission: Directorate General for Enterprise and Industry*

Fernando Sanchez Gomez
Guardia Civil

Gordon Sarlet
European Affairs Advisor, *Thales Airborne Systems Centre Charles Nungesser*

Timothee Sautter
Consultant, *European Public Policy Advisers (EPPA)*

Jan-Willem Scheijgrond
Director, Government Affairs, *Hewlett Packard*

Lizanne Scott
Senior Director, Government Relations Europe, *Motorola*

Radu Serban
Minister Counsellor, *Embassy of Romania to Belgium*

Alexander Skoryukov
Senior Counsellor, *Mission of the Russian Federation to the EU*

John Smith
Manager, Strategy & Planning - Governments/Public Sector, *Hewlett-Packard Company*

Petr Solsky
Second Secretary, Judicial Cooperation, Civil Protection, *Permanent Representation of the Czech Republic to the EU*

Ivica Stehlikova
Office of the Counter-Terrorism Coordinator, *Council of the European Union*

Martin Suenson
Executive Officer, *European Petroleum Industry Association (EUROPIA)*

Nevin Sungur
Brussels Correspondent, *NTV*

Petr Svacina
Terrorism Co-ordinator, *Ministry of Foreign Affairs, Czech Republic*

Brooks Tigner
EU / NATO Correspondent, *Defense News*

Milos Todorovic
First Secretary, *Mission of Serbia to the EU*

Emrush Ujkani
Senior Officer for EU Affairs, *Agency for European Integration/Kosovo Government*

Leendert Van Bochoven
Partner Public Sector, European Defence/Network Centric Operations, *IBM*

René van Dijk
Risk Policy Unit, Crisis Control Department, *Ministry of Interior and Kingdom Relations, the Netherlands*

Ernst van Hoek
Director European Affairs, *TNO-Defence Research*

Fan Weimin
Counsellor, *Mission of China to the EU*

Christine Wenzel
EU Government Relations Manager, Global Communications, *SAP AG*

Rachel Winks
Director, EU and NATO Relations, *Boeing International*

Laura-Kate Wilson
European Affairs Department, *European Aeronautic Defence and Space Company (EADS)*

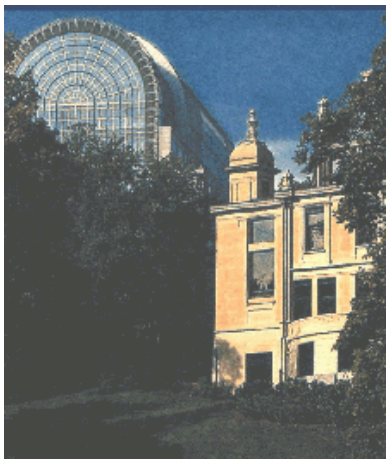
Tineke Zuurbier
TABD EU Assistant Director, *The Transatlantic Business Dialogue (TABD)*

SDA IN 2006

19 JANUARY Book presentation **UTILITY OF FORCE: THE ART OF WAR IN THE MODERN WORLD** **WITH GENERAL SIR RUPERT SMITH AND JAVIER SOLANA**	**30 JANUARY** Monthly Roundtable **IS A TRANSATLANTIC DEFENCE INDUSTRY INCREASINGLY ON THE CARDS?**
20 FEBRUARY Monthly Roundtable **CHARTING THE DEVELOPMENT AND USES OF NETWORK CENTRIC CAPABILITIES**	**24 APRIL** Monthly Roundtable **BORDERS & PEOPLE: THE LIBERTY AND SECURITY BALANCE**
28 APRIL Monthly Roundtable **THE ISSUES SHAPING ASIAN SECURITY**	**30 MAY** Annual Security Conference **PROTECTING EUROPE'S CITIZENS: POLICIES FOR ENHANCING SECURITY IN THE EU**
13 JUNE Expert Seminar **EUROPE'S LONG-TERM VISION OF THE DEFENCE ENVIRONMENT IN 2025: SHARP OR FUZZY?**	**20 SEPTEMBER** Expert Seminar **ADVISORY BOARD MEETING**
2 OCTOBER Monthly Roundtable **DEFENDING EUROPE'S VULNERABLE INFRASTRUCTURE**	**16 OCTOBER** Monthly Roundtable and Space Reporting Group **IS EUROPE SERIOUS ABOUT SPACE AND SECURITY?**
6 NOVEMBER Annual Conference **GLOBAL NATO: OVERDUE OR OVERSTRETCH?**	
13 NOVEMBER Evening debate with the Finnish Presidency and European Defence Agency **EUROPEAN TECHNOLOGICAL AND DEFENCE INDUSTRIAL BASE**	**7 DECEMBER** Monthly Roundtable **THE PRIVATE SECURITY PHENOMENON: POLICY IMPLICATIONS AND ISSUES**
13 DECEMBER Dinner discussion on Pandemic Flu with **DIRECTOR GENERAL FOR HEALTH AND CONSUMER PROTECTION ROBERT MADELIN**	**DECEMBER** Press Dinner with **EUROPEAN COMMISSIONER FOR ENTERPRISE AND INDUSTRY GÜNTER VERHEUGEN**

EU COMMISSIONER FRANCO FRATTINI ADDRESS THE SDA'S ANNUAL SECURITY CONFERENCE

ABOUT THE SECURITY & DEFENCE AGENDA



The Security & Defence Agenda (SDA) is the only specialist Brussels-based think-tank where EU institutions, NATO, national governments, industry, specialised and international media, think tanks, academia and NGOs gather to discuss the future of European and transatlantic security and defence policies in Europe and worldwide.

Building on the combined expertise and authority of those involved in our meetings, the SDA gives greater prominence to the complex questions of how EU and NATO policies can complement one another, and how transatlantic challenges such as terrorism and Weapons of Mass Destruction can be met.

By offering a high-level and neutral platform for debate, the SDA sets out to clarify policy positions, stimulate discussion and ensure a wider understanding of defence and security issues by the press and public opinion.

SDA PATRONS

Javier Solana, EU High Representative for the Common and Foreign Security Policy
Jaap de Hoop Scheffer, Secretary General of NATO
Franco Frattini, European Commissioner for Justice, Freedom and Security
Benita Ferrero Waldner, European Commissioner for External Relations and European Neighbourhood Policy

RECENT SDA ACTIVITIES

HIGHLIGHTS FROM SPRING 2006

General Sir Rupert Smith and Javier Solana at SDA's "Utility of Force" debate 19 January 2006

Franco Frattini, EU Commissioner for Justice, Security and Freedom talks to Giuseppe Orsi CEO of AgustaWestland and Denis Ranque CEO of Thales at SDA's annual security conference 30 May

Atlantic Rendez Vous transatlantic satellite debate organised in conjunction with SDA's annual security conference 30 May 2006

Asian Security Roundtable gathers experts to discuss priorities and responses 28 April 2006

THE SECURITY & DEFENCE AGENDA WOULD LIKE TO THANK ITS PARTNERS AND MEMBERS FOR THEIR SUPPORT IN MAKING THE SDA A SUCCESS

Mission of the Russian Federation to the EU

Mission of the US to NATO

Delegation of the Netherlands to NATO

Ministry of National Defence, Turkey

Centre for Studies in Security and Diplomacy
University of Birmingham

Interested in joining the SDA? Please contact LINDA KARVINEN:
Tel:+32 (0)2 737 9148
Fax: +32 (0)2 736 3216
Email : linda.karvinen@securitydefenceagenda.org

A *Security & Defence Agenda* Roundtable Report

Photos: Frédéric Remouchamps, Keops

SECURITY & DEFENCE AGENDA (SDA)

Bibliothèque Solvay, Park Léopold, 137 rue Belliard, B-1040, Brussels, Belgium
Tel: +32 (0)2 737 91 48 Fax: +32 (0)2 736 32 16 E-mail: info@securitydefenceagenda.org
www.securitydefenceagenda.org