NEW DEFENCE AGENDA

A Neutral Platform for discussing NATO and EU Defence and Security Policies

President: Eduardo Serra

Patrons: Javier Solana, Jaap de Hoop Scheffer
Franco Frattini and Benita Ferrero-Waldner

STRATEGIC PRIORITIES FOR PROTECTING EUROPE'S INFRASTRUCTURE AGAINST TERRORISM

Moderated by Giles Merritt, Director, New Defence Agenda
Rapporteur: John Chapman

Monday, 27 June, 2005
Bibliothèque Solvay, Brussels

NEW DEFENCE AGENDA
Bibliothèque Solvay, Parc Léopold, 137 rue Belliard, B-1040, Brussels, Belgium
T: +32 (0)2 737 91 48 F: +32 (0)2 736 32 16 E: info@newdefenceagenda.org
www.newdefenceagenda.org

NEW DEFENCE AGENDA

CONTENTS:

INTRODUCTION

Ten days after this NDA Roundtable on the vulnerability of critical infrastructures to terrorist attack, London's transport system was hit by four near-simultaneous bomb attacks.

The London death toll, at just over 50, was mercifully low in comparison to Madrid's loss of almost 200 people in the Atocha railway station bombings of March 2004, to say nothing of New York's 9/11 casualty list of about 100 times as many deaths. But if London underlined the importance of chance in determining the loss of life, the bombings there have also given fresh impetus to efforts to better coordinate national counter-terrorism measures.

All three of major terrorist attacks were, there seems no room for doubt, carried out by fanatics operating under the general banner of Al Qaida. They emphasise yet again that if anti-terrorism protection and emergency response is fundamentally local, intelligence gathering and the sharing of information is only feasible if it is international.

In the months ahead, the NDA will be further strengthening its programme of homeland security discussions and related events.

Giles Merritt
Director
New Defence Agenda

TIME TO TELL IT HOW IT IS!

The last NDA roundtable before the summer break examined Europe's plans to counter terrorist attacks on its critical infrastructure. At one stage, NDA Director Giles Merritt was moved to ask if the EU's citizens should be on their guard or whether they should feel relaxed. Later Merritt observed that the terrorists appeared to have a window of opportunity to mount attacks while the EU finalised its plans. Those interventions told the tale of the latest NDA deliberations. The Commission was developing comprehensive plans and clarifying who would do exactly what, and when they would be doing it.

Merritt concluded that he had not heard a coherent political message and he called on politicians to explain to the public what governments (and institutions) were doing to make Europe safer. The EU's citizens had to be engaged and had to be given the facts. If there was an added value in protecting the "European homeland", as opposed to relying on national initiatives, then it must be clearly explained to one and all.

Painting a comprehensive picture of the Commission's plans, Magnus Ovilius emphasised the responsibility of the member states in controlling the process and being responsible for "hard" issues, such as funding the necessary upgrades to critical infrastructure. He reasoned that "bureaucrats in Brussels should not dictate what is to be done on the ground", a comment that was perhaps a sign of the times.

During the debate, it was noted that although the US was spending much more on defence and security than Europe, there were doubts as to the wisdom of such expenditure. Allen Green argued that the US could not continue to spend on defence at the current rate. Ovilius took the opportunity to defend Europe's "cost aware" approach, whilst acknowledging that this would take an additional amount of time.

The clock indeed was ticking. Europe should have plans in place and it should be understood who was responsible for mounting protection, what the threats actually were and the best ways of combating attacks – on people and on infrastructure.

Not that the roundtable was short of ideas. They came thick and fast. There had to be:

- more engagement with the private sector, a vital factor
- greater interaction between European institutions and member states
- more analysis on the key inter-dependencies (information exchange and energy) and the impact that any interruption would have on business
- more co-operation and collaboration
- rapid alert systems in the key sectors

But there was a lack of clarity in the overall actions to be taken and no message for public consumption. Ovilius emphasised that the Commission was "doing a lot". Certainly the list of its activities (defining the scope of the exercise, identifying critical infrastructures, analysing the potential damage costs to the economy, developing a Commission Crisis Centre) was impressive but subsidiarity seemed to be the name of the game.

On the subject of whether Europe had a "homeland security industry", only the Commission's Herbert von Bose was certain. It did not exist. He argued that policymakers still placed national interests first. As for markets, van Bose did not see one for security products. Many sectors were involved and he wanted more cross-sector collaboration. The European Homeland Security Association's Christian Sommade concluded that "small steps" were necessary. If the terrorists were listening, they would be sleeping easily in the their beds.

SESSION I – WHAT NEEDS TO BE DONE AND HOW MUCH WILL IT COST?

Introducing the debate, NDA Director Giles Merritt observed that while there had been several national assessments, there had been no attempt to define Europe's infrastructure vulnerability in total. In the fight against terrorism, he wanted to know if the strength of the EU in total was greater than the sum of the individual member states. Where was the EU's added value?

Brigadier General Ian Abbott, Chief of Policy and Plans Division, European Union Military Staff

Brigadier General Abbott examined the phrase "critical national infrastructure" in detail. Looking at each word in turn, the Brigadier General drew some conclusions:

- Critical: What is critical? The psychological impact could be greater than that caused by the actual casualties, i.e. more people die on the road than are killed by terrorists, but the reaction is minimal. One tends to take note of attacks that have used new or novel methods. In addition, children and old people are the most vulnerable and climatic factors cannot be overlooked (cold in winter, lack of water in summer, wind direction, etc.) as these can increase the effects.
- National: Nations have new priorities. Due to the reliance on international networks, no nation can stand alone. The focus is no longer on war, but on trade. Just-in-time has replaced just-in-case and there are minimal reserves held in supermarkets, gas holders, petrol stations, etc. Society has become more vulnerable.
- Infrastructure: Not all nations view infrastructure in the same way. No universal model exists that defines critical infrastructure, but essential elements should include the generation and distribution of energy, health maintenance, the detection of resulting threats, water & sanitation control, and telecomms / information control.

Moving onto planning for the restoration of the status quo, the Brigadier General's advice was to ignore the (many) scenarios and concentrate on the effects of an attack. He suggested giving priority to maintaining normality by, for example, ensuring that homes, schools and cinemas were as important as industry. The attitude of "business as usual" should prevail. The financial networks (ATMs etc.) and the media should also be on the list of "high priority" items.

Overall, Brigadier General Abbott wanted remedial plans to:

- ensure that maintenance in the elected government was maintained
- bring about a return to normality as soon as possible
- focus on the effects (of an attack)

"We need a public information campaign that strikes a balance between fearing and forgetting".

Brigadier General Ian Abbott

Jose Antonio Hoyos Perez, Policy Officer, Directorate-General for Energy and Transport, European Commission

Hoyos Perez noted that the decision to act at the EU level in the protection of critical infrastructures was taken (June 2004) by Member States' Heads of States and Governments in the aftermath of the Madrid attack recognizing the existence of a European dimension of the problem, in areas such as energy, where the creation of a single market of energy establishes a predominance of the European approach.

Hoyos Perez focused on the energy-related aspects of the EU's critical infrastructures, explaining that this was part of the European Commission's wider initiative EPCIP[1]. The Commission is currently conducting a consultative process to define the actions to be taken prior to issuing a communication by the end of 2005. Reviewing the plans to develop a single market for electricity & gas by 2007, Hoyos Perez acknowledged that this would mean more cross-border flows (to increase security of supply). In parallel, this meant that attacks on the network's weakest links could have a greater cross-border impact. He also indicated that the introduction of a single market for energy would necessitate the development of a "single voice" for the whole community, one that included suppliers such as Russia, Norway and North Africa.

Hoyos Perez defined DG TREN's key issues as: the identification of critical energy infrastructures (based on national perceptions), the content of the strategy (a full or restricted view of threats), the engagement of the private sector and full cooperation of the member states. Opinions were being collected with the aim of agreeing a methodology for the identification of critical infrastructures and a definition of the minimum level of protection required – on an ongoing basis.

EPCIP

<u>Benefits</u>

- Promotion of an ongoing forum that balances competition and information sensitivity with enhanced security
- Provision of information to partners on the nature of specific threats
- Development of standards by CEN (the European Committee for Standardisation) where necessary

<u>Goals</u>

- To develop equal and adequate levels of protective security (of critical infrastructures) across the EU on an ongoing basis
- To minimise single points of failure
- To develop rapid recovery arrangements

<u>Measures of success</u> (EPCIP must)

- Develop inventories of critical infrastructures
- Reduce the likelihood of incidents impacting critical infrastructures
- Establish a common approach to tackling the problem via public-private partnerships

[1] EPCIP: the creation of a European Programme for Critical Infrastructure Protection consolidating and bringing together the Commission capability to advise and assist in critical infrastructure protection measures.

Magnus Ovilius, Senior Administrator, Directorate-General for Justice, Freedom and Security, European Commission

Magnus Ovilius gave a complete account of the EPCIP framework (necessary to guarantee the protection of the EU's critical infrastructure) under consideration by the European Commission. This would be presented by the end of 2005 for initial implementation next year. Ovilius stressed that this programme would also cover the impact of accidents, natural disasters, hacking and criminal activities as well as terrorist threats. Importantly, he also emphasised that responsibility for the protection of critical infrastructures would remain in the hands of owners and operators (in the member states).

Ovilius commented that in order to facilitate the exchange of information on shared threats and vulnerabilities, the Commission would create the CIWIN network[2], a rapid alert system that would promote best practices and formulate appropriate measures.

Responsibilities

For Ovilius, the involvement of the private sector was vital. The owners and operators would be responsible for the actual physical protection. They would develop plans and undertake regular inspections of facilities. The member states would therefore control the process while the European Commission would ensure equal and adequate implementation across the EU.

The EPCIP programme would also define to industry the benefits of taking measures to reduce the risk to critical infrastructures. The Commission would aim to minimise any impact on competitiveness and Ovilius stressed that a cost-benefit analysis should include the need to maintain (trade) markets and a stable stock market in the event of attacks. For their part, member states' authorities should interact and identify inter-dependencies, especially in key areas such as energy and information exchange (the Internet and related areas). These sectors cut across many others and it was necessary to develop business contingency plans.

> "Bureaucrats in Brussels should not dictate what is to be done on the ground (in the member states)".
>
> Magnus Ovilius

Ovilius added that member states had the responsibility to identify critical infrastructures, identify threats, reduce vulnerabilities and identify the source of attacks (post incident). He stressed the need for co-operation, coordination and communication nationally and at the EU level where relevant. Subsidiarity was the name of the game.

As for the players (owners, operators, regulators, professional bodies, etc.), Ovilius wanted, above all else, co-operation with governments in regard to security. The Commission would also be producing a legislative proposal on data protection but this would be outside the scope of the EPCIP.

2 The EU Critical Infrastructure Warning Information Network (CIWIN) - to assist Member States, and owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Common principles on critical infrastructure protection (as defined by DG Justice, Freedom and Security):

- Responsibility for managing risk stays with owners and operators
- EPCIP's success relies on inter-dependencies (business, member states' authorities, etc.)
- EPCIP requires a consistent partnership (member states and owners, public & private)
- Sharing information between partners will reduce risk
- EPCIP will help raise awareness of risks and roles to be taken to protect infrastructures
- Member states should examine inter-dependencies (and thereby enhance protection)
- Member states should continuously test plans (with other stakeholders)
- Member states should engage in EU cross-border co-operation
- Member states and the Commission should promote R&D (to agreed mutual standards)
- The Commission will develop further actions (common standards, inspections, feasibility studies, dissemination of information, regulations, etc.) where necessary

Funding

Ovilius explained that the Commission had prepared (under the planned financial perspectives for 2007 – 2013) a programme for the "prevention, preparedness and consequence management of terrorism". While national, regional and local authorities would be invited to participate in the financing, Ovilius stated that the Commission would cover "the majority of the funding". He added that the Commission would undertake certain actions (see table above) but that upgrading of the infrastructure hardware for security purposes remained with member states.

Explaining that the Commission's funding would be in the region of €140 million - "sufficient for the soft issues", Ovilius added that this would be supported by structural funds for sectoral programmes, such as the environment, energy, public health and transport. Loans could also be available (for infrastructure upgrades) from financial institutions and this would be examined with the European Investment Bank. Finally he added the Commission would consider making available an annual amount of €250 million (2007 – 2013) for research into practical strategies for risk mitigation.

"The EPCIP programme should explain the benefits for industry of taking measures to reduce risk".

Magnus Ovilius

Kevin Rosner, Senior Level External Expert to NATO and Senior Fellow, Institute for the Analysis of Global Security (IAGS), Washington DC

Kevin Rosner focused on the energy security issue. He reasoned that the global energy system was being endangered by the fear of terrorism, the growing demand, limitations on the use of nuclear power and "a misguided set of policies by some EU member states" that was increasing dependency on the Russian federation.

Rosner argued that energy security was not a stand-alone issue. It had to be addressed in a trans-national context. He argued that NATO was ideally placed to lead contingency planning and strategies to be used in the event of emergencies in its area of responsibility. As the Alliance's security was dependent on its response to issues such as terrorism, sabotage and the continuing flow of vital resources, Rosner said it was incumbent on NATO to debate and determine its role in mitigating risks to energy supply[3]. There were "political, economic, military and social aspects to this situation".

As for strategic priorities, Rosner reminded the roundtable that it would be wise to engage the technology and security providers in a

[3] Rosner announced a forum on this issue to be hosted by the NATO Science Division to be held in Prague in November 2005.

comprehensive effort to assess risks. He warned that terrorists could easily migrate from Iraq ("armed with specialist knowledge") and that Osama Bin Laden had a declared a holy war on the oil industry – "the Crusader nations' artery".

> "It is naive at best and dangerous at worst to believe that terrorists will remain limited to Iraq".
>
> Kevin Rosner

After pointing out some of the problems in protecting Europe's supplies of oil and gas (65% of Europe's oil passes through the Mediterranean, there were no standards for physical security, the lack of early warning systems) Rosner returned to the issue of dependency on Russian oil. He argued that this was expected to increase as Europe's imports would increase significantly from the current figure of 50%, much of it to be supplied from the Russian Federation. He added that the new EU member states were taking 80% of their oil supplies and 75% of their gas supplies from Russia. Rosner saw this as a serious issue as the dependency on energy supplies was increasing at a time when Russia's commitment to democracy and the rule of law was being called into question.

In conclusion, Rosner called for cross-border security standards, cross-border early warning systems, a genuine debate between interested parties (service providers, NATO, etc) and a reconsideration on the role of nuclear energy (as some EU member states were placing environment issues ahead of security of their citizens).

First session – Q&As

Public information systems

Posing the fist question, Giles Merritt asked if we should be reassuring the public or alerting it to the risk of terrorist attacks on the EU's critical infrastructure. Magnus Ovilius answered that one. He stated that a common strategy was being developed so that communication was the same across the EU member states. The message should be reliable, correct and promote confidence within the public. There also remained the issue of who should issue such messages.

> "A misguided set of policies is deepening the energy insecurity of some EU member states by increasing imports and dependency on the Russian federation".
>
> Kevin Rosner

What should be protected?

In terms of protecting the critical infrastructure, the European Parliament's Adviser Ernst Guelcher argued that it was impossible to protect every aspect and asked if there was any point in protecting anything (as the terrorists would simply switch their targets).

Ernst & Young's Glenn Schoen followed up on Guelcher's point by asking if either the EU or NATO had analysed why terrorists attacked certain targets[4], and pointed out that Al Qaida had introduced a relatively new tactic of attacking critical targets despite the high security that was in place.

Brigadier General Abbott agreed that there was no way to protect all the targets and that a new model – based on preparedness – was needed. He added that terrorists simply needed to raise fears, e.g. about the controllability of nuclear power, in order to have dramatic psychological and financial effects.

[4] Schoen added that the authorities in Europe had thwarted 19 major attacks since 9/11. Merritt later asked if he should be alarmed or reassured by this information.

Funding

Merritt wanted to know the cost of protecting Europe's infrastructure and who would be picking up the bill. In terms of costs vs. benefits, he added that 9/11 had had a significant cost in terms of the effect on stock markets, air traffic, tourism, etc.

McKenna Long & Aldridge's Allen Green had some figures from the Homeland Security Research Corporation. This analysis stated that the US currently accounted for 52% of the global homeland security market, but that the US figure would only grow by 12% (in 2005-2015) compared with a 16% annual growth elsewhere (EU, China, India, etc.). Green saw the global market expanding from $26 billion to $178 billion by 2015.

Green was keen to know who would fund this investment in Europe and how the public and private elements of the expenditure would be spilt.

On the subject of funding, Jose Antonio Hoyos Perez explained that solving the problem of how public and private organisations would contribute towards the cost of paying for counter terrorism measures was equivalent to solving the Gordian Knot. Noting some of the complexities involved, Hoyos Perez added that the costs were dependent on the definition of critical infrastructure at both national and EU levels. Green countered with a supplementary question as to whether there would be funding at the EU level as well as at the national levels. Hoyos Perez felt that it was too premature to be definitive on that matter and emphasised that funding depended on the Member States' approval of the Financial Perspective of 2007-2013.

This was too much for Merritt who asked if the terrorists had a "window of opportunity" to attack Europe's critical infrastructure while the funding issue was resolved. Hoyos Perez defended his position by saying that it was simply a matter of seeing if financial rules had to be changed, as structural funds might be available.

Giving comprehensive responses to several questions, Ovilius took up the cudgels on behalf of the Commission. He insisted that much work was being undertaken and security was being increased. Ovilius also defended the "cost aware" approach of the EU, whilst acknowledging that doing the job properly – in collaboration with the private sector - would take a significant amount of time. Once critical weaknesses had been identified, it would be necessary to link up with the intelligence authorities to decide where the money would be spent to generate the maximum effect.

The role of the EU Military staff

After hearing Brigadier General Abbott, Defense News' Brooks Tigner wanted clarification as to what steps the European Union Military Staff was taking in response to the terrorist threats against critical infrastructure. Abbott stated that the EU Military Staff was working on counter terrorism measures with the European Commission through the member states. When pressed further, the Brigadier insisted that the member states still had responsibility for security. It was business as usual.

What data will be kept?

Eden Intelligence's Giulio Thuburn reasoned that collecting information (on weaknesses) was easy. He wanted to know how that information would be used in the long-term and if it could be the basis for a European homeland security database. EIS' Brian Beary asked if anyone was drawing up a list of Europe's critical infrastructure and, if so, would it be made public.

On the subject of a "super" database in Brussels, Ovilius thought this was, a) unnecessary and b) unmanageable. This data was needed by the member states. They would keep it and it would never be made public. However a list of critical infrastructures would be drawn up with the Commission focusing on infrastructures with a cross-border impact where it could add value (e.g. coordination role across borders).

Is Europe's power in the right place?

Jose Manuel Gonzalez Cotano was concerned that the inter-governmental institutions and transparency-national institutions lacked sufficient power to dissuade terrorists from attacking critical infrastructures. How could a more powerful framework be developed in Europe? Ovilius felt that the European institutions had sufficient power but they had chosen to leave the main responsibility in the hands of the member states on the basis of subsidiarity.

Learning from Y2K

The European Commission's Andrew Denison, speaking as an individual, asked if lessons had been learnt (in terms of the planned investment on counter terrorism) from the enormous amount of expenditure on the Y2K issue. Had anyone done a cost-benefit analysis to see if that had been money well spent? Ovilius did not think that a thorough analysis of the Y2K had been performed but, if necessary, immediate funding was available.

Added value from the European Commission

Merritt came back on the alleged $62 billion being spent in the US on homeland security. As the Commission was ideally placed to assess the shortcomings of European civil emergency services (cross-border, backup, etc.), he suggested it should estimate what was needed to develop a European homeland security policy – so Europe could have a funding target.

Ovilius thought this was taking the discussion into another area and he took the opportunity to discuss the creation of a European Commission Crisis Centre that would coordinate and link 12 existing rapid alert systems (health, radiological alerts, etc.) under an umbrella system ARGUS. Links to the aforementioned CIWIN and a planned law enforcement network would be added at a later date. A proposal on the crisis centre would be presented by July 2006.

Has the Cold War ended?

Tigner had been confused by Rosner's criticism of the EU's policy on energy imports from Russia, as it was a not a model of democracy and the rule of law. Referring to the US's high rate of imports (said to be over 50%) and its dependency on countries such as Saudi Arabia, Tigner asked Rosner which alternative model (of energy supply) should be followed by the EU. Kevin Rosner agreed that the Cold War was over but he insisted there were 217,000 kilometres of pipelines in Russia and most of the energy products moving from East to West were Russian products. He felt Russia wanted to work with the EU (EU-Russia Dialogue, the Energy Charter, the NATO-Russia Council) but the issue was not receiving sufficient attention, as it was "off the radar".

Ovilius agreed that pipelines were vital (within the EU and its neighbours) and that adequate security had to be addressed. There had to be global compatible solutions that were developed in a coordinated way. While admitting the complexity of the issues, he added that private industry was reasonably keen to get involved.

SESSION 2: IS EUROPE DEVELOPING A "HOMELAND DEFENCE INDUSTRY"?

NDA Director Giles Merritt was also in charge for the second session that looked at the prospects for Europe's "Homeland Defence Industry". Merritt wanted to hear about new technologies, the Commission's views on the role of research and innovation in the security sector and more on the likely costs.

Ulf Dahlsten, Director, Directorate for Emerging Technologies and Infrastructure, Directorate-General for Information Society and Media, European Commission

Ulf Dahlsten's focussed his intervention on two complementary aspects: The first one is the need for increasing support to dual use research on emerging technologies for the mutual benefit of security/defence and private sectors. The second one is the necessity for defence and security to play their leading role in driving innovation in Europe as done in the US. First, he pointed out that the frontier between security and defence are somehow 'blurred' nowadays. With a nod in the direction of the US, he noted that on that side of the Atlantic, the defence and security industries were driving innovation with their strong focus on dual use of technology for both the public (defence & security) and private (commercial) sectors and with technology procurement. That model historically successfully adopted in some Member States now needs to be put in place at European level if we want to compete. To illustrate the opportunities in emerging technologies in Europe, Dahlsten took two examples : robotics and communication (middleware, grids) and collaborative systems. In all such areas, Dahlsten stressed that in order to make innovation and generate growth, three groups of actors needed to closely cooperate towards common goals:

- the research community as generator of idea and technology
- the future owners/producer of the technology as driver of innovation
- and the future users/buyers as critical success factor for the take-up of any innovation

This innovation triangle of stakeholders needs to be supported by appropriate and coordinated financial funding at Member States and at European level commensurate with the risk associated with research and innovation. This is the only way to transform ideas into growth (and jobs) – the EU's priority.

Robotics

A new generation of networked robotic systems able to collaborate towards common goals are emerging thanks to the progress in a number of technologies and in their integration. This new generation open new avenues for applications in the traditional manufacturing industry, in defence and security but also in the service industry. Applications listed includes: industrial, medical, service (vacuum cleaners, lawn mowers, etc.), space and security & defence. Dahlsten explained that under this top application layer, there are clear needs for more technology developments of common building blocks (development of sensors, development of navigation systems in complex environments, development of communications systems, development of learning and cooperating capabilities etc.). In the robotics sector, the community of stakeholders is getting in place around the following group of actors:

- EURON (the European Robotics Network[5]) – Network of key actors from the research community
- EUROP – the industry initiative[6] that are driving the 'Technology platform' currently being created and that regroup established and emerging European companies in industrial and service robotics. Including some actors from the security and defence sector such as Thales or Safran (ex Sagem group).

In terms of funding, robotics is one of the key priorities of the ICT domain within the 7th European Framework Programme for R&D currently under discussion. Strong interest for robotic has also been expressed recently in particular from the six countries strongly involved in funding defence research.

However, Dahlsten stressed that there was a need to identify the first buyers for the

[5] Details at http://www.euron.org/
[6] Details at http://www.euron.org/europ/index.htm

applications being researched. Listing possible avenues for exploration, he looked to the European Space Agency (ESA), to the creation of an EU equivalent to the US' Defense Advanced Research Projects Agency (DARPA) or of an EU Homeland Defence Advanced Research Projects Agency (possibly called HARPA). In support of this approach, he gave the example of DARPA that had been built on the basis of some initial project research. The idea was to start small and grow.

Communication systems (middleware & grids)

In a similar way, Dahlsten stressed the latest development in the area of communication and collaborative systems with the renewed co-operation getting in place in this sector between the different actors:

- The CoreGRID project[7] for example is a network of excellence gathering the main actors from the research community in the area of grid and middleware.
- The SEASIDE initiative is a technology platform under creation that regroups all the major industrial actors in grid, software and IT services with the view to establish a common vision and research agenda and ensure its implementation.
- In terms of user or early adopter, the research community with the eInfrastructure initiative is one example of traditionally high demanding users (they were at the origin of the web!) that drive innovation in this domain. In the industrial sector, the SIMDAT project is involving early users from various sectors such as the automotive, the aeronautics or the pharmaceutical sectors.

With applications on both the research infrastructure side and in the commercial sector, Dahlsten saw this as an area that could develop rapidly.

One objective of such communication systems is to enable people to work and collaborate together to accomplish complex or simple tasks in a safe and secure way in any kind media and knowledge rich environments. . This has direct application in the defence sector for example in the domain of command field control. This is a critical capability when forces from different nations (with different communication systems) are deployed, so that they could work together and cooperate in a secured environment. Other areas of application are civil security protection, risk prevention or crisis management.

Internet – the next generation

Dahlsten concluded with a few words on convergence and on the deployment of IpV6[8]. IpV6 is a key technology to support the deployment of next generation of internet. It provides 'quasi' unlimited internet address spaces and more security features than current IpV4 protocol. Dahlsten acknowledged that the communications market place (voice, video, television, etc.) was moving to IP (Internet Protocol) and that only regulations in the EU telecommunications sector were slowing down the deployment of the next generation of the Internet within Europe. The take-up of the next generation of internet is rapid in China, Korea and Japan. Take-up of IpV6 is in particular critical for Asia due to the shortage of Internet addresses with current IPv4 protocol. The US defence sector has announced his intent to move to IpV6 by 2008 and would probably create a special agency to oversee Ipv6's implementation.

[7] CoreGRID brings together a European critical mass of well-known experts in GRID and P2P research allowing to compete with research and development in US and Japan. (see http://www.coregrid.net/).

[8] IPv6 (Internet Protocol Version 6) is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4"), which is now nearly 20 years old. IPv4 is beginning to have problems and there is a shortage of IPv4 addresses, needed by all new machines added to the Web.

Allen Green, Senior Partner, McKenna Long & Aldridge

Allen Green was interested in the participation of the private sector in the creation of the European homeland security market. He explained that this had been one of the main driving forces in the creation of the US homeland security industry. That led him to the litigious aspects of the defence & security industry in the U.S., where many companies had been frightened to get involved in the development of "counter terrorism" products for those very reasons, i.e. if there was a successful terrorist attack, then massive lawsuits alleging the company's products or services had "failed" likely would follow.

In the US, the response had been to create the SAFETY Act (Support Anti-Terrorism by Fostering Effective Technologies Act)[9], which provided that a company could submit details of products and projects to the Department of Homeland Security. Once certified, that company would have protection regardless of whether its product was provided or its services performed under government or commercial contracts. This encouraged US investment and ownership.

Green noted that during the day's discussions EC officials had discussed the critical need for the private sector to take a lead role in developing a secure infrastructure. Green argued that the same concerns would be present in Europe. He added that the consequences for failure were huge – within society and also in terms of the economic viability of private sector companies. He recommended that member states and the Commission work together to develop a process and regulation similar to the SAFETY Act, so that companies engaging in these public/private initiatives would be protected.

[9] For more on this, see (http://www.ebglaw.com/article_887.html).

Stephen Orosz, Director, Civil Emergency Planning Consultancy (CEPCON) and former Deputy Assistant Secretary General for Civil Emergency Planning, NATO Planning, NATO

Stephen Orosz argued that a homeland security market already existed in Europe, as part of a global industry. Moving on to priorities, he asked what actions should be taken and by whom. Orosz felt that it would not be sufficient to rely on industry. Companies were essentially driven by commercial considerations and voluntary steps might not be enough. Therefore, governments might need to compel industries to take certain actions.

Here, Orosz recommended a balanced approach that treated companies equally (regardless of location). He did, however, acknowledge that such a process would take time. Orosz gave an example of public-private co-operation with the World Customs Organization's decision to implement comprehensive standards in the fight against terrorism (inspections at ports of departure instead of ports of arrival, and preferential treatment for private importers who tighten security).

After giving an example that showed that public-private cooperation did not always work[10], Orosz gave the argument for industry involvement, saying it was essential in order to ensure private sector buy-in, as they would be responsible for implementation. As for the public sector, co-operation was needed among governments and agencies at all levels: local, regional and national. He then added other agencies to the mix (intelligence, law enforcement and diplomacy for example),

[10] US Homeland Security Secretary Chertoff recently announced a change of course regarding anti-terror rules for chemical plants in the US. A voluntary system had been put in place that encouraged chemical plant owners to conduct self-assessments and take steps to eliminate vulnerabilities. However, after only 1,100 of the 15,000 US plants with large amounts of dangerous chemicals participated in the voluntary program, Chertoff concluded that voluntary efforts alone were inadequate and called upon Congress to adopt federal standards.

together with co-operation between the civilian and defence sectors.

Calling for openness, even if this benefited adversaries, Orosz suggested that strategic partnerships would ensure the adequate flow of appropriate information for both public and private sector actors. He concluded with a look at the policies needed in Europe, and added that the EU Council and the Commission were doing a good job on "soft" systems and procedures. He called for the EU to continue to work to reduce the threat in the agricultural sector and also take a lead in the "Achilles Heel" of the critical infrastructure remit, i.e. the public health sector. Here he argued that no nation had any "surge capacity" and saw a role for the EU, working closely with the WHO.

Christian Sommade, President, European Homeland Security Association

Christian Sommade spoke on behalf of the newly formed European Homeland Security Association. He described the current security market, one worth $260 billion on a worldwide basis ($113 billion in the US and $90 billion in Europe), and then looked at the prospects of a "homeland security" market in Europe. He felt this was more likely due to the increased political involvement ("a new vision") and the new regulations in the field.

Looking at the issues, Sommade reasoned that regulatory progress was somewhat fragmented and it was not obvious how "homeland security" initiatives would be funded. He then turned to several of the requirements of the new industry. These included:

- the need to guard against identity theft
- the need to improve security in the public health sector
- civil protection (more complex as the EU was spending much less than the US)
- new technologies, where there was a lack of investment in R&D in most EU countries
- standards, that did not exist for homeland security
- R&D within the EU – with its insignificant funding compared with the US

Sommade did not see this as a totally new industry, but rather one where five sectors were combining: the defence industry (with declining budgets in the last decade), the hi-tech industry, bio and public health, security industry (growing) and SMEs (who were looking for R&D funding).

Asking if a real homeland security industry could be developed in Europe, he hoped that a 9/11-type incident would not be a trigger. Instead he called for common EU security funding. Research funding was insufficient and Sommade wanted dual-use research on civil protection (both against terrorist attacks and natural disasters) and security (seen as a burden in the citizens' eyes). He also stressed the need for security to be visible at the local level, and concluded with a call for the creation of a Homeland Security Academy (where best practices and concepts could be shared).

Herbert von Bose, Head of Unit, Preparatory action for security research, Directorate-General for Enterprise and Industry, European Commission

Herbert von Bose argued that Sommade's call for the creation of a Homeland Security Academy was premature. He didn't believe that the term "homeland Europe" had any resonance. Politicians spoke about their nations. This meant that there were 25 security markets, rather than one.

> "We have the elements of a security industry but they have not been consolidated in Europe."
>
> Herbert von Bose

He personally favoured the creation of a European homeland security market. However, to move forward, there had to be a demonstration of the advantages to be gained by operating in a trans-national, European or global context. Examples listed by von Bose included: border security, anti-terrorism, organised crime, protection of critical infrastructure and crisis management. In this way, Europe would be showing added-value. Moving on to actions, within a public-private partnership (users and suppliers), von Bose was brutally honest. He said that a European market for security products did not exist and the interested parties had to work together to define the requirements (e.g.

where was a common European response required?).

On the subject of industries, he also argued that no single industry existed. Many different sectors played a role in the security market (s), e.g. IT, biotechnology, pharmaceuticals, SMEs etc. Putting that in context, von Bose said that the biotechnology and pharmaceutical industries had only a limited participation in the Preparatory Action in the field of Security Research (PASR), which had limited funding[11]. This compared with significant involvement from the traditional defence companies, the IT industry and SMEs.

Overall, von Bose saw all the elements of a security industry existing in Europe but there was a need for consolidation. He stressed the importance of research[12] and added that many companies were now active in the security sector. Ending on the importance of international co-operation, von Bose argued that this global problem had first to be met by a public-public partnership (Europe and US) before private companies were involved. That would be the most pragmatic approach. He also foresaw an increase in PASR funding from 2007. For von Bose, the most critical element was collaboration – networking should be emphasised at both the intra-European and transatlantic levels.

[11] In order to prepare the ground for security research in FP7, the Commission has launched a 'Preparatory Action in the field of Security Research', spanning a period of three years (2004-2006) with a planned budget of € 54 million.
[12] In parallel, a European Security Research Advisory Board (ESRAB) has been set up. It is composed of industrialists, academics and public and private users.

SECOND SESSION – Q&AS

Getting industry involved

The Commission's Jacques Bus supported von Bose and added that his unit (ICT for Trust and Security) was spending approximately 35 million per annum on activities related to critical infrastructure protection. Bus considered this to be insufficient, saying his unit aimed to spend between € 50 million and 70 million in future (research on critical infrastructure protection, inter-dependencies of systems etc.).

Giles Merritt took the opportunity to argue that although major companies were involved in "homeland security", there did not appear to be a high level of preparedness (or dissuasion) in Europe. Merritt's idea was to introduce tax incentives to ensure that private sector companies were motivated to be involved and critical infrastructure protected. He did not see voluntary actions being successful.

Allen Green came back to the rather fuzzy difference between defence and security. He explained that most of the money being spent in the US was "classic defence" budget money. Green also argued that most companies, such as Boeing, had divisions that were aimed at both security and defence.

Stephen Orosz did not agree with Merritt that Europe had not done much in terms of being prepared. He argued that Europe had started late, in comparison with the US, and had made good progress. As for tax incentives in Europe, he did not see national governments cutting their revenues. Orosz agreed with Green that profit would be the prime motivator in the private sector, and he added that money had to be shifted from the classic defence arena to the security sector.

Herbert Von Bose focused on the carrot (money on the table) and stick (regulations) options that the Commission possessed. He said the former was the preferred approach, as the latter was extremely unpopular, with taxes in particular raising levels of nervous tension. Although progress was slow (and the funding insufficient), von Bose said it was going in the right direction.

What's the security agenda?

Merritt asked the panel to consider whether the current status of European industry co-operation on security was matching the activities in the more classic defence area, where he felt "Europe has come a long way in the last five or 10 years". He wondered if a Bannerman plan was on the horizon.

Ulf Dahlsten was in full agreement with Merritt, but he felt that it was too early to create a true European security agenda. National activities were still predominant and he could only see small steps being taken that would encourage others to improve the speed of progress. Christian Sommade felt that time was running out and he saw the need to raise public opinion. Sommade wanted activities to start at the local level (to get public support) before more grandiose plans could be developed.

The Commission's Leo Koolen intervened to ask for an in-depth investigation into Europe's security situation. It had been said (by Donald Rumsfeld) that Europe was spending half of the amount spent by the US but only had 10% of its capabilities. Assuming that was correct, Koolen wanted to know the reasons and called for the political commitment to hold a fundamental debate on current expenditure levels (and the associated waste).

Koolen was also concerned about the liberalisation of the telecommunications markets and the impact that it could have on the ability of governments to adequately protect critical information infrastructure. Company management in the industry was now focused on profit and the stock market, and less attention would be paid to infrastructure protection.

Orosz agreed that the US was spending more in the US but he asked if the money was being well spent. Speculating on the actual value of $1 billion frigates and $25 million aircraft, Orosz therefore asked how superior did the US need to be. Turning to Europe, Orosz said the picture was fragmenting and budgets were tightening. However, the security picture was changing and new priorities had to be set.

Green agreed with Koolen. He also argued that the US could not to continue to spend money (on defence and security) at the current rate.

Green saw the US "trying to do more with less (dollars)" in future.

End of session

Merritt wrapped up the session by defining what the European institutions should be trying to do in this post-Constitution era. He suggested they should be explaining to the citizens of Europe what they were doing to make Europe a safer place to live.

Merritt was not hearing a coherent political message and he called on politicians to establish a real dialogue with the public so that they could explain what governments (and institutions) were doing to make Europe safer. Merritt felt that would be a win-win situation for institutions and citizens alike.

PROGRAMME:

SESSION 1 – WHAT NEEDS TO BE DONE AND HOW MUCH WILL IT COST?

Heightened preparedness is the best way to discourage terrorist attacks on Europe's national landmarks, business and infrastructural nerve centres. In the US, the cost of upgrading first response emergency services to deter non-nuclear terrorist attack is put at $62bn over the coming five years. What needs to be done in Europe, with what cooperative mechanisms and from where will the money come? Are there lessons to be learned from the US experience?

Moderator: Giles Merritt, Director, New Defence Agenda

- Ian Abbott, Director, Policy and Plans Division, European Union Military Staff
- Jose Antonio Hoyos Perez, Policy Officer, Directorate-General for Energy and Transport, European Commission
- Magnus Ovilius, Senior Administrator, Directorate-General for Justice, Freedom and Security, European Commission
- Kevin Rosner, Senior Fellow, Institute for the Analysis of Global Security (IAGS) and UK Defence Academy

SESSION 2 – IS EUROPE DEVELOPING A "HOMELAND DEFENCE INDUSTRY"?

The leading European and American defence and security-related companies are now competing hard to develop new anti-terrorism technologies. Will this create a 'homeland security industry' that specializes in countering new threats? What priority areas should industry be identifying, and what sort of public-private partnerships can be developed as a form of burden sharing? What policies should the EU and its members governments be developing to increase R&D and to give more support to innovative SMEs?

Moderator: Giles Merritt, Director, New Defence Agenda

- Ulf Dahlsten, Director, Directorate for Emerging Technologies and Infrastructure, Directorate-General for Information Society and Media, European Commission
- Allen Green, Senior Partner, McKenna Long & Aldridge
- Stephen Orosz, Director, Civil Emergency Planning Consultancy (CEPCON) and former Deputy Assistant Secretary General for Civil Emergency Planning, NATO
- Christian Sommade, President, European Homeland Security Association
- Herbert von Bose, Head of Unit, Preparatory action for security research, Directorate-General for Enterprise and Industry, European Commission

LIST OF PARTICIPANTS, 27 JUNE 2005

Ian Abbott Chief of Policy and Plans Division	European Union Military Staff
Massimo Amadei Policy & Plans Division	European Union Military Staff
Robert Anger Consultant	Fleishman-Hillard
Fathi Ayoub Economic Counsellor	Mission of Libya to the EU
Adrienne Baughman NATO Correspondent	Jane's Defence Weekly
Brian Beary Journalist, Justice and Home Affairs, Internal Market	Europe Information Service (EIS)
Robert Bell Senior Vice President European Business	Science Applications International Corporation (SAIC)
Ilana Bet-El Op-Ed Editor	European Voice
Hans Joerg Brandenburger Delegate	Thales
Hartmut Bühl Senior Executive Consultant NATO	European Aeronautic Defence and Space Company (EADS)
Jacques Bus Head of Unit, ICT for Trust and Security	European Commission, DG for Information Society and Media
Geert Cami Managing Director	New Defence Agenda
Ergam Camözü Adviser to the WEU and WEAG NADREP	Mission of Turkey to the EU
Giuseppe Carta Senior Vice President, Strategic Marketing	OTO Melara SpA - Finmeccanica
John Chapman Rapporteur	New Defence Agenda
Ulf Dahlsten Director, Emerging Technologies and Infrastructures Applications	European Commission, DG for Information Society and Media
Danny de Temmerman Desk Officer, Policy and Legal Affairs	European Commission, DG for Justice, Freedom and Security
Jill S. Dekker-Bellamy Bio-Defence Consultant	New Defence Agenda
Andrew Denison Detached National Expert	European Commission, DG for External Relations
Marc Devisscher Press & External Communications Manager	European Chemical Industry Council (CEFIC)

Andrey Dorofeev First Secretary	Mission of the Russian Federation to the EU
Julien Feugier European Affairs Manager	European Aeronautic Defence and Space Company (EADS)
Anne Fichtel	
Nicholas Fiorenza Brussels Correspondent	Armed Forces Journal Europe
Maria Laura Franciosi Correspondent	Avvenire
Fatima Ghardi Project Manager	Ecole Nationale d'Administration, Paris
Bill Giles Director General Europe	BAE Systems
Jose Manuel Gonzalez Cotano	
Don Goshen Assistant to Head of Israeli Mission of Defence	Embassy of Israel to Belgium
Drora Goshen-Meskin Director, R&D and Business Development	European Advanced Technologies
Allen B. Green Senior Partner	McKenna Long & Aldridge
Franck Greverie Vice President Strategy	Thales
Michael Grimes Consultant	New Defence Agenda
Ernst Guelcher Advisor Peace and Human Rights	European Parliament, Green Group/European Free Alliance
Gustav E. Gustenau Deputy of the Commissioner for Strategic Studies, Bureau for Security Policy	Ministry of National Defence, Austria
Rainer Hellmann Journalist	Fuchsbriefe
Jessica Henderson Project Manager	New Defence Agenda
Arnauld Hibon Vice-President, Director EU Affairs	Eurocopter
Jose Antonio Hoyos Perez Principal Administrator	European Commission, DG for Energy and Transport
Meeri-Maria Jaarva Director, State Building and Democracy	Crisis Management Initiative (CMI)
Tomwit Jarnson Minister Counsellor	Mission of Thailand to the EU
Kari Kahiluoto Deputy Head of Mission	Delegation of Finland to NATO

Lars Karlén Vice President Marketing	Ericsson Microwave Systems
Linda Karvinen Project Manager	New Defence Agenda
Robyn Kessler Commercial Officer	Mission of the United States of America to the EU
Laszlo Kiss Transnational issues Task Force	European Union Military Staff
Spyros Konidaris Advisor to the Deputy Director General	European Commission, DG for Information Society and Media
Leo Koolen Administrator, Policy Developer	European Commission, DG for Information Society and Media
Andrzej Kopytko Senior Specialist of Department of Defence Affairs	Ministry of Infrastructure, Poland
Victor Kulagin Counsellor	Embassy of the Russian Federation to Belgium
Christophe Lamfalussy Journaliste, Politique extérieure	La Libre Belgique
Jacob Langvad Security and Defence Editor	EurActiv.com
Bart Lateur Student	Ghent University
Anna Löfgren Project Assistant	New Defence Agenda
Javanshir Mammadov Counsellor	Mission of Azerbaijan to NATO
E.I Margherita Consultant	Rafael
Guy Meguer Solutions Marketing Director- Homeland Security	European Aeronautic Defence and Space Company (EADS)
Giles Merritt Director	New Defence Agenda
Mark Miller Business Development, Supply Chain Security	COTECNA Inspections
Uwe Moeller Head of Office	Deutsches Zentrum für Raum- und Luftfahrt (DLR)
Stephen C. Orosz Director	Civil Emergency Planning Consulancy (CEPCON)
Magnus Ovilius Senior Administrator	European Commission, DG for Justice, Freedom and Security
Agnes Page Chargeé de Mission	Thales

Pablo Perez-Illana Project Officer	European Commission, DG for Research
Olympios Raptis Security & Defence Technical	AeroSpace and Defence Industries Association of Europe (ASD)
Luigi Rebuffi Director for European Affairs	Thales
Kevin Rosner Senior Fellow	Institute for the Analysis of Global Security (IAGS)
Piotr Rydzkowski Desk Officer	European Commission, DG for Justice, Freedom and Security
Timothee Sautter Consultant	European Public Policy Advisers (EPPA)
Daniel R. Schaubacher Representative to the European Institutions	European Baha'i Business Forum
Glenn Schoen Senior Manager, Ernst & Young Security and Integrity Services	Ernst & Young
Radu Serban Minister Counsellor	Embassy of Romania to Belgium
Alexander Skoryukov Senior Counsellor	Mission of the Russian Federation to the EU
Haim Soffer Vice President Business Development	OIP Sensor Systems
Christian Sommade President	European Homeland Security Association (EHSA)
Iréne Svensson Senior Vice President, Corporate Communications and Public Affairs	Group Saab
Giulio Thuburn Director, Energy Security Research Division	Eden Intelligence
Brooks Tigner EU Correspondent	Defense News
Herbert Von Bose Head of Unit, Preparatory action for security research	European Commission, DG for Enterprise and Industry
Hans-Juergen Wieland Head External Relations	European Aeronautic Defence and Space Company (EADS)
Mojtaha Zahedi Third Secretary	Embassy of Iran to Belgium
Lorenzo Zito International Affairs Department	Finmeccanica

About the New Defence Agenda

The New Defence Agenda (NDA) has become established as the only regular Brussels-based forum where political figures and journalists gather to discuss the future of European and transatlantic defence and security policies.

The aim of the NDA is not to replicate more academic research-based projects but to give greater prominence to the complex questions of how EU and NATO policies can complement one another, and how transatlantic challenges such as terrorism and WMD can be met.


La Bibliothèque Solvay

Bringing clarity and new ideas to the rapidly-changing defence and security policy scene has been the NDA's aim from its beginning. NDA's activities range from monthly roundtables and international conferences to reports and discussion papers, all of which attract high-level speakers and authors and institutional, governmental and industry support.

One of our prime objectives is to raise the profile of defence and security issues among the Brussels-based international press. To encourage more in-depth coverage of these topics, the NDA holds regular, informal dinners for journalists with high profile decision makers.

Recent speakers and participants include
Benoît d'Aboville, Ambassador, Permanent Delegation of France to NATO; Gijs de Vries, Counter-terrorism Coordinator, Council of the EU; Richard Falkenrath, Research Fellow, Brookings Institution and former Deputy Homeland Security Advisor to the US President; Franco Frattini, Commissioner for Justice, Freedom and Security, European Commission; Bill Giles, Director General, Europe, BAe Systems; Vecdi Gönül, National Defence Minister, Turkey; Scott A. Harris, President, Lockheed Martin International; Patrick Hennessey, Director, DG Enterprise, European Commission; Hilmar Linnenkamp, Deputy Chief Executive, European Defence Agency; Alessandro Minuto Rizzo, Deputy Secretary General, NATO; Sergei Ordzhonikidze, Director General of the United Nations Office in Geneva; Zonghuai Qaio, Vice Foreign Minister, Ministry of Foreign Affairs, China; George Robertson, Former Secretary General, North Atlantic Treaty Organisation; Gary Titley, MEP, Committee on Industry, External Trade, Research and Energy, European Parliament; Michel Troubetzkoy, Senior Vice President, Director for Relations with European Institutions, EADS; Günter Verheugen, Commissioner for Enterprise and Industry, European Commission; Antonio Vitorino, former Commissioner for Justice and Home Affairs, European Commission; Karl von Wogau, Chairman, Subcommittee on Defence and Security, European Parliament,

"[NATO] An Alliance in which Europe and North America are consulting every day on the key security issues before them. Acting together, in the field, to defend our shared security... Because in a dangerous world, business as usual is not an option"
NATO Secretary General Jaap de Hoop Scheffer, NDA Conference 17 May 2004

"Homeland Security = a concerted, comprehensive and nationwide effort to prevent future terrorist attacks, to protect the most vulnerable targets against future terrorist attacks and to be ready to respond against possible attacks and minimize loss of life and damage if such attacks occur" Richard Falkenrath, former Deputy Assistant to the President and Deputy Homeland Security Advisor, 17 November 2003 NDA Conference

"The agency should generate ideas and speak the truth to defence ministers."
Nick Witney, Chief Executive, European Defence Agency 28 April 2004 NDA Press Dinner

"There is an opportunity for Europe to take advantage of the US's investment by issuing collaborative programmes – paid for to a certain extent by the US taxpayer. The European Defence Agency could foster transatlantic cooperation rather than follow more traditional approaches"
Scott Harris, President Continental Europe, Lockheed Martin, 28 April 2004 NDA Press Dinner

THE NEW DEFENCE AGENDA WOULD LIKE TO THANK ITS PARTNERS AND MEMBERS FOR THEIR SUPPORT IN MAKING THE NDA A SUCCESS

Ministry of National Defence, Turkey

Ministry of National Defence, Romania

Mission of the Russian Federation to EU

NEW DEFENCE AGENDA

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@newdefenceagenda.org
www.newdefenceagenda.org