SDA Monthly Roundtable

Assessing the Cyber Security Threat

Bibliothèque Solvay, Brussels

SDA
SECURITY & DEFENCE AGENDA

A *Security & Defence Agenda* Report
Rapporteur: John Chapman
Photos: David Plas
Year of publication: 2008

SECURITY & 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@securitydefenceagenda.org W: www.securitydefenceagenda.org

Contents

Executive Summary

Following a fascinating debate that ranged from bullet-proof hosting to onion-routing, the conclusion had to be that the cyber security threat was evolving rapidly and was touching all aspects of society. Its political importance is also increasing and in a cyber society that "has no rules or borders", according to Estonia's Minister of Defence Jaak Aaviksoo, there is a need for improved coordination at the highest level.

Estonian Minister of Defence Jaak Aaviksoo

Indeed, the London School of Economics and Political Science's Professor Peter Sommer highlighted the need for such cooperation, although that had been his message for some years. In the aftermath of the alleged denial of service attacks on his country, Minister Aaviksoo, said they had been a threat his country's economy. Russia's Ambassador to the EU, Vladimir Chizhov, focused on the increasing number of websites that incited people to act as terrorists, many of which he said were hosted in the EU.

It was left to the Council of Europe's Alexander Seger to remind everyone that the Council had developed a Convention on Cyber-Crime, which also covered 'cyber attacks', as experienced by Estonia. He was confident that if a crime involved the use of a computer in any way, then the convention did apply. However, he added that only 22 of the 43 signatories had so far ratified the 2001 treaty, including just 13 of the EU's Member States. As Seger added, even the best treaty in the world would not work without cooperation.

Council of Europe's Alexander Seger

Background

Cyber attacks, such as the spring 2007 alleged cyber attack on Estonia made headlines across the world. The US Department of Homeland Security has staged major exercises such as 'Cyber Storm' to study the potential economic and national security impact of cyber warfare. The illegal use of cyberspace is, some say, a $100 billion business, bigger than the worldwide drug trade. With governments and the business world increasingly concerned that cyber threats are outpacing cyber defences, there are many questions unanswered. The recent SDA session on cyber security set out to find solutions to the puzzle.

> "With the best treaty in the world, you still need the political commitment to cooperate."
>
> Alexander Seger

Professor Peter Sommer, London School of Economics

The Debate

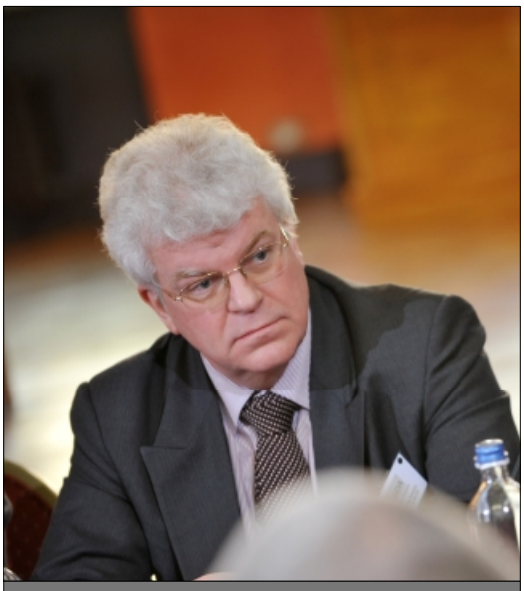
Setting the Scene

The cyber security threat is hard to define. As Estonia's Minister of Defence Jaak Aaviksoo stated, "there are no rules and no borders in cyber space". The London School of Economics and Political Science's Professor Peter Sommer, who argued that diagnosing cyber-related events was difficult, swiftly took up that point. Listing the various terms – "cyber warfare", "cyber espionage", "cyber weaponry", "cyber terrorism", "cyber crime" – Professor Sommer insisted that discipline was required when discussing the subject.

This report examines the various cyber topics discussed at the SDA event, and reviews the solutions placed on the table. Professor Sommer was right to request discipline, but that is not easy in cyber space. He also told the SDA to be "wary of statistics", so treat this document with caution.

Cyber Attacks

Most cyber attacks tend to be linked to denials of service, and can be made for political or criminal purposes. Giving an overview of the alleged cyber attacks on Estonia in 2007, Aaviksoo stated that he did not place particular importance on the details of who, what, where. He was more concerned about the perception that national security had been under attack from



Russian Ambassador to the EU Vladimir Chizhov

cyber space. There had been no attempts to access classified databases. However, Minister Aaviksoo insisted that the Estonian public, in a country where 90% of tax declarations and bank transactions are online, had thought that their accustomed way of life was under threat. Aaviksoo also placed the importance on the defence of the interface between technology and people – "because people depend on the integrity of data".

Richard Troy, Policy Officer, DG Justice, Freedom and Security, European Commission

Minister Aaviksoo added that Estonia had quickly mobilised defences after the first attacks, due to the existence of a *Computer Emergency Response Team*, established by an informal network of the key players. As for explanations, the authorities had found "no smoking gun" but the attacks had been linked to the relocation of the Soviet War Memorial in Tallinn and the "different waves of attacks took place according to Moscow time".

> "There are no footprints or fingerprints in cyber space.
>
> Jaak Aaviksoo"

Russia's Ambassador to the EU, Vladimir Chizhov argued that, paradoxically, the most advanced nations, in introducing computer technology, were also the most vulnerable to cyber attacks. To back his argument, Ambassador Chizhov claimed that the US had the most websites contaminated with malware, with a third of the world's total, followed by China (31%) and Russia with 9%. Note: But see table – origin of malware - from Symantec.

Professor Sommer insisted that identifying hackers was extremely difficult. As an example, the Professor said an attack on a US Research Laboratory had been linked to North Korea or Latvia, but had actually come from a 16-year-old boy in London, Techniques existed, he added, such as

"botnets and onion routing" that could hide the origin of the attack. Another problem identified by the Professor was that the Internet held details of weaknesses that could be used against itself, for the purposes of causing denials of service, crime or terrorism.

Cyber Terrorism

Websites can, of course, be used to incite people to take part in illegal, criminal or political acts. Ambassador Chizhov had more concern about such 'cyber terrorism' than about cyber attacks. He claimed that the number of websites that were inciting people to commit acts of violence was growing (now at +/- 5,000 according to the Ambassador). His answer was public-private cooperation, but Ambassador Chizhov highlighted fact that the EU often took no action against websites that incited violence and that were based in its Member States.

> "…we are adapting to an environment that is at once borderless and in a state of constant evolution.
>
> Richard Troy

DG Justice, Freedom and Security's Richard Troy described the Commission's approach to combating cyber crime as pragmatic, specifically targeting improvements in:

- capacity building, e.g. law enforcement, training, etc.
- operations, e.g. public-private cooperation, civil society involvement

Member of the European Parliament, Bill Newton Dunn

> "We want to crack the problem but we are not sure how to do it.
>
> Bill Newton Dunn

- education of the public
- international coordination of activities

Last year, the Commission announced the creation of the European Security Research and Innovation Forum (ESRIF), which aims to bring public and private expertise together to lay the ground for a security research agenda. This would contribute to developing the European Security Research Agenda over the medium to long-term.

Cyber Crime

Cyber crime is a growing business. Two of the main types of such crime are phishing and pharming: phishing schemes use e-mails to make people go to a phony website, whereas pharming relates to the set-up of a fraudulent website that contains copies of pages from a legitimate website in order to capture confidential information from

Director, NATO Headquarters Consultation, Command and Control Staff (NHQC3S), Major General Georges D'hollander

users.

Touching on cyber crime, Ambassador Chizhov said Russia had been promoting cyber crime legislation in line with global trends since 1997, and was ahead of most countries. But he agreed there was no legal definition of cyber crime and that political will was needed to combat such crime. His solution was to bring together the various elements of the international community under the auspices of the UN. However, Professor Sommer suggested the vital aspect was the "willingness to cooperate". The Mission of China to the EU's Deyi Gao said China was making efforts to prohibit cyber crime and was doing its best to ensure cyber security. This included the police launching campaigns against cyber crime. He saw the need for international cooperation and collaboration.

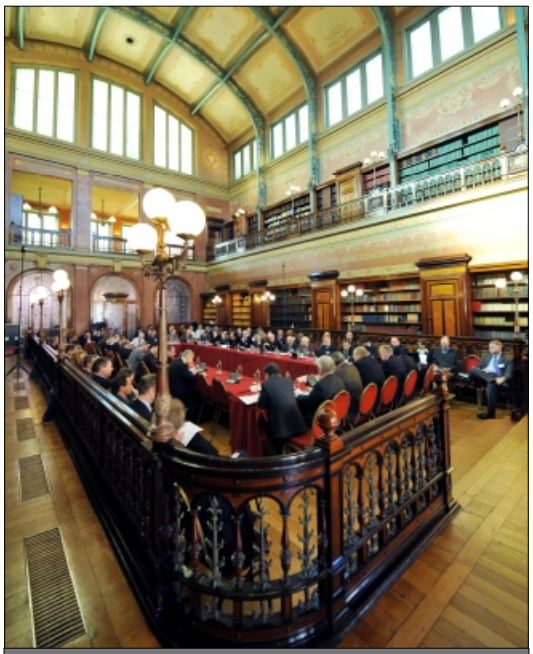
Deyi Gao, Political Counsellor, Mission of China to the EU

> "There are notorious sites that have survived several crackdowns … and have risen again in other countries, including EU countries.
>
> Vladimir Chizhov"

Troy illustrated the complex nature of the cyber-crime environment by referring to the practice of bullet-proof hosting, whereby anyone could buy a service that enabled them to offer illegal and criminal services under the mask of anonymity. Using such facilities, criminal organisations were involved in identify theft and online child abuse. MEP Bill Newton Dunn broadened the discussion regarding cyber crime by referring to the exponential increase in counterfeiting of CDs, DVDs and even fake pharmaceuticals. However, Newton Dunn did not feel that the public was particularly concerned about cyber crime and that it would take a "real crisis to attract public attention".

Alexander Seger, Head of Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, insisted that 99.9% of computer users were acting legitimately and he did not want counter measures to infringe the human rights of such users. His solution was for everyone to sign the council's convention (see solutions).

> "We need to be disciplined in our use of language in this arena as a necessary precursor to disciplined analysis and the search for solutions. Much work has already been done by non-military security agencies."
>
> Professor Peter Sommer



The roundtable during the debate.

Solutions

NATO's Plans

NATO intends to enhance its overall cyber defence policy. Director, NATO Headquarters Consultation, Command and Control Staff (NHQC3S), Maj. Gen. Georges D'hollander said the initial focus would be on defending NATO's own infrastructure against cyber attacks. He also stressed the need for standards and the search for government and industry best practices – this was being done in league with the Network Centric Operations Industry Consortium (NCOIC) working on "network enabled capability". D'hollander added that the implementation of the policy would speed up the response capability of systems, personnel and processes in the defence against cyber attacks and that a cyber defence authority would be developed to manage cyber defence capabilities so they could act quickly.

> "NATO and UN working together could bring added-value in the fight against cyber attacks."
>
> Major General Georges D'hollander

Reviewing the Internet Itself

DG InfoSoc's Head of Unit Jacques Bus moved the attention to the Internet itself, saying it was "almost broken". Adding that many people were re-thinking the future of the Internet, Bus said there must be a technical solution

to creating safe borders, and hence increasing security, but he recognised the political and social pressures.

> "Interoperability is vital and we are working with industry on best practices and standards."
>
> Major General Georges D'hollander

D'hollander, however, was against the creation of borders, as this would affect NATO's need for information sharing. Professor Sommer was not in agreement with Bus either, as he felt the imposition of new borders would be against the trend of globalisation. The Professor was against re-inventing the wheel and was in favour of having a greater emphasis on the current proposals on international harmonisation, which were included in initiatives such as the Council of Europe's Convention on Cyber Crime.

The Council of Europe's Convention on Cyber Crime

Seger stressed that existing opportunities were not being sufficiently exploited. Focusing on the council's convention, open for signature since 2001, it has been signed by 43 countries. Adding that it was the only internationally binding treaty in the area, it covered denial-of-service attacks, data interference, computer-related fraud, child pornography, intellectual-property rights, procedural rights (to ensure more effective investigation), international cooperation and the need to balance civil rights privacy against security needs.

Despite the convention being ratified by many eastern European countries and the US, signed by Canada, Japan and South Africa, accession under way by Costa Rica, Mexico and the Philippines, Seger said that 14 of the EU's Member States had not yet done so. However, he remained optimistic, and he wanted efforts to be expanded to the rest of the world.

Importantly, Aaviksoo was concerned that the convention focused on crime and did not cover attacks that went beyond attempts at personal gain and had more political motivation. He hinted that new instruments might be needed. Seger disagreed, adding that the situation had been reviewed following the attacks on Estonia and that the convention did cover attacks against confidentiality, integrity and the availability of systems, including system interference. However, he acknowledged that the best treaty in the world would not work without sufficient cooperation.

> "Inventing new borders goes against the trend of globalisation."
>
> Professor Peter Sommer

Segers added that the convention did not mention issues such as money laundering and human trafficking, but that if a crime involved a computer (even if that was just sending an email) then the convention's procedural measures could be invoked.

Press Coverage - A Selection

"There are notorious sites that have survived several crackdowns… and have risen again in other countries, including European countries."

Russian ambassador to the EU Vladimir Chizhov
Eupolitix.com

"Events in cyberspace can affect our life at a large scale in the moment we perceive them as a national security threat."

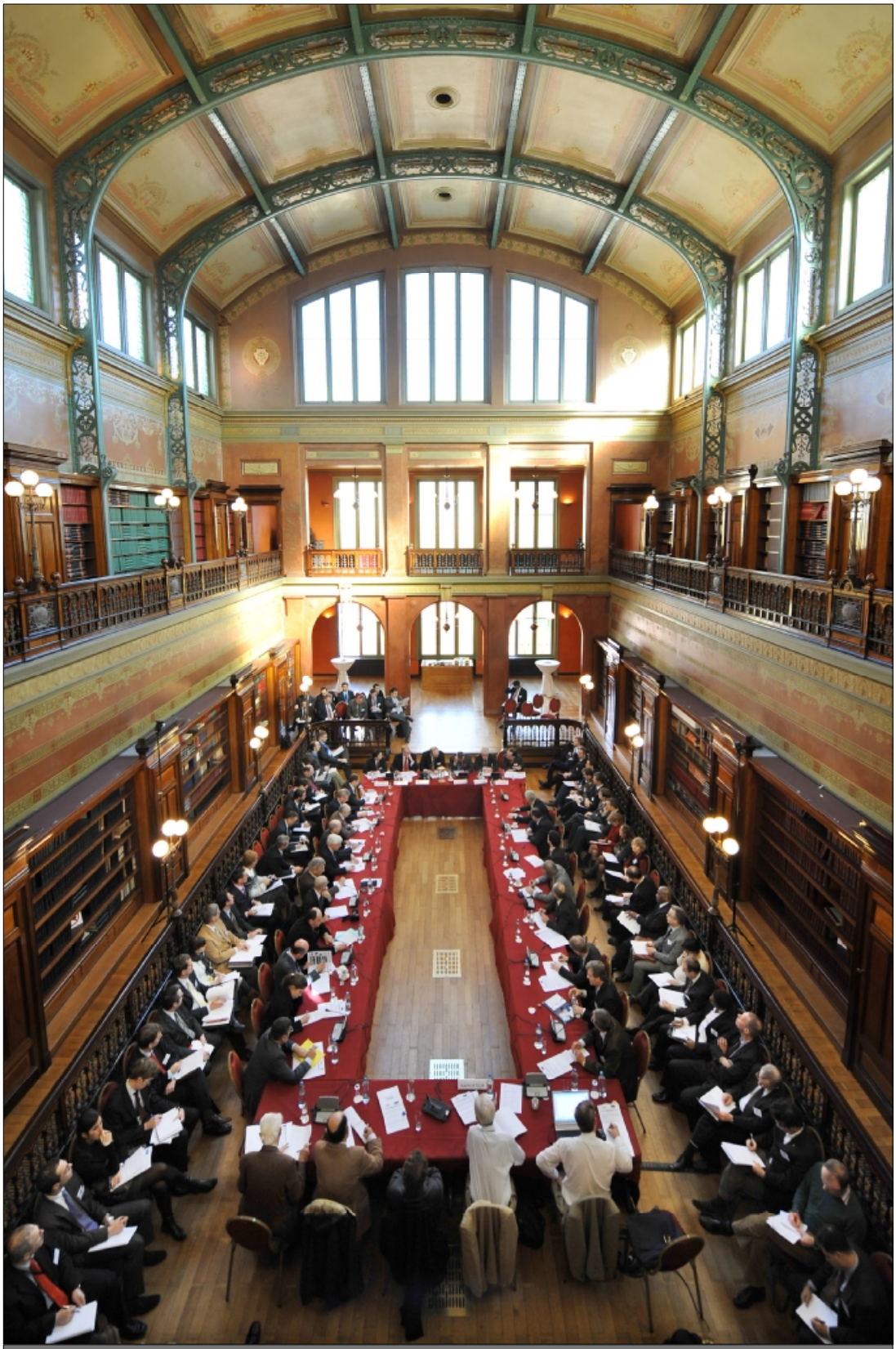
Estonian Denfence Minister Jaak Aaviksoo
Euractiv.com

"Governments can certainly do more to cooperate more with each other, to criminalise certain conduct... strengthen the confidence in cyberspace."

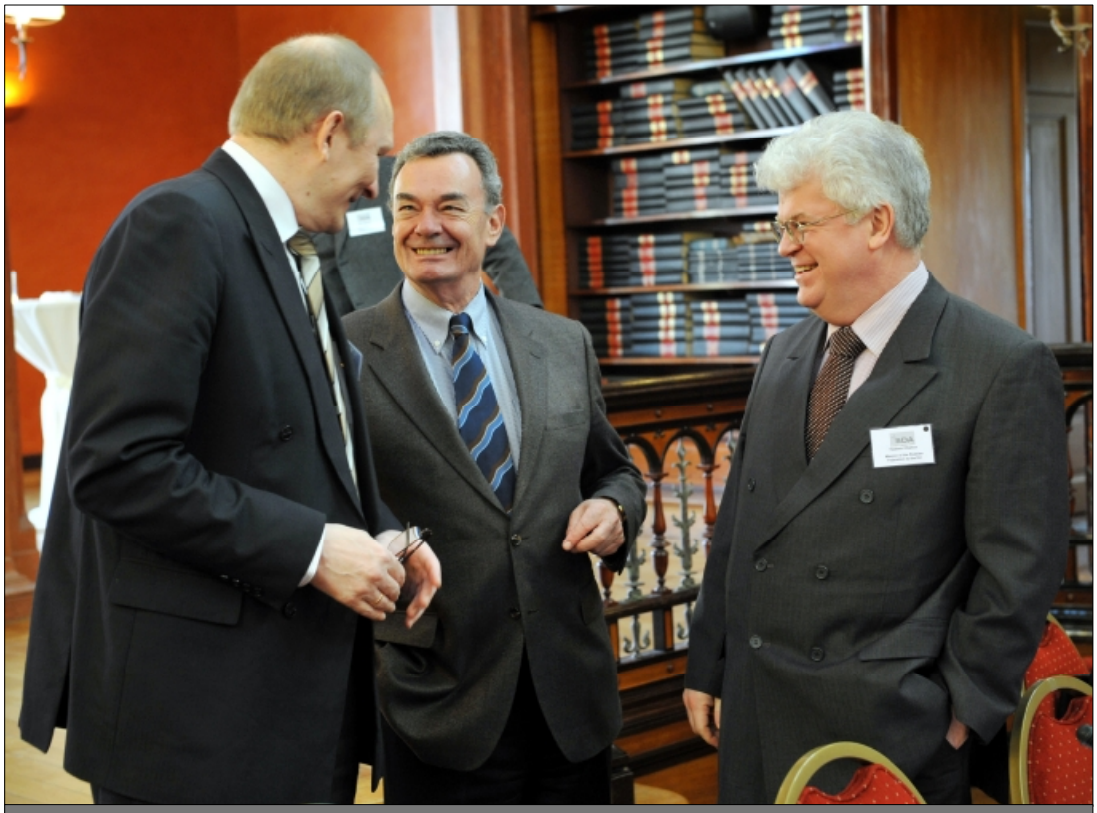
Council of Europe's Alexander Seger
Euronews

"The first priority in the field of cyber crime is to discipline the way we talk about the subject, also because the diagnosis of events is very difficult. We have to always be sure that attacks are brought about by real terrorists and not crazy teenagers."

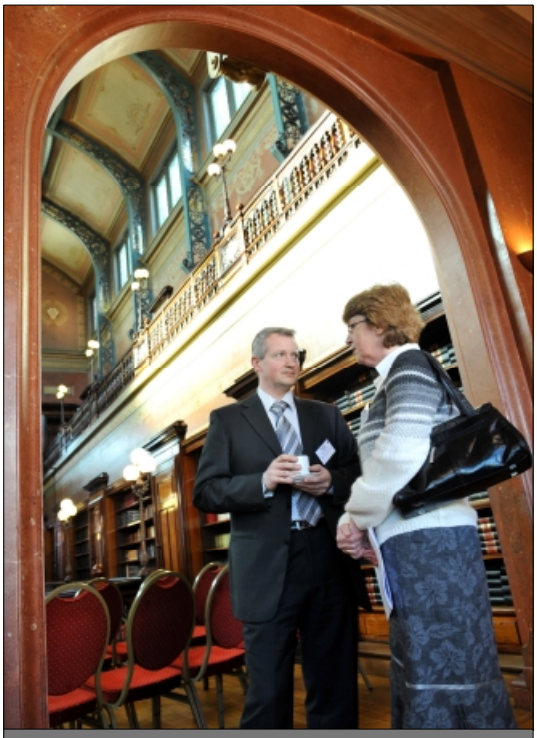
Professor Peter Sommer, London School of Economics (LSE)
Euractiv.com



Morning session of the roundtable as seen from above.



(From left) Jaak Aaviksoo, SDA Director Giles Merritt and Vladimir Chizhov talk prior to the roundtable.



Participants discuss the issues during an intermission.

A participant talks to speaker Deyi Gao.

List of Participants

Jaak Aaviksoo
Minister
Ministry of Defence, Estonia

Muzaffer Akyildirim
Defence Counsellor
Mission of Turkey to the EU

Josu Alberdi
Liaison Police Officer
Basque Country Home Office

Oleg Aleksandrov
First Secretary
Embassy of Ukraine to Belgium

Valérie Andrianavaly
Network and Information Security Officer
European Commission, Directorate General for Information Society & Media

Avivit Bar-Ilan
First Secretary - NATO Relations
Mission of Israel to the EU

Jacquelyn Bednarz
Attaché, Department of Homeland Security
Mission of the United States of America to the EU

Thomas Bondiguel
Chargé de mission (attaché au point de contact think tanks)
Permanent Representation of France to the EU

Bart Bonner
Defence Advisor
Ministry of Defence, Belgium

Björn Brenner
Analyst
Swedish National Defence College (SNDC) Försvarshögskolan

René Bullinga
NCOIC NATO IPT Chairman
European Aeronautic Defence and Space Company (EADS)

Jacques Bus
Head of Unit, ICT for Trust and Security
European Commission, Directorate General for Information Society & Media

Geert Cami
Managing Director

Sergio Cantone
Brussels Correspondent

Gianluca Cazzaniga
Correspondent
Italian Defence Review

Pierre Chambe
Chargée de Mission, Mission des Affaires Étrangers
Permanent Representation of France to the EU

John Chapman
Rapporteur
Security & Defence Agenda (SDA)

Patrick Chatard Moulin
Official, Defence issues
Council of the European Union, Directorate General for External and Politico-Military Affairs

Vladimir Chizhov
Ambassador
Mission of the Russian Federation to the EU

Mark Clark
V.P. European Region, Business Development
Raytheon International, Europe

Sarah Collins
Journalist
The Parliament Magazine

Jaak Cuppens
Belux Country Manager
F5 Networks

Miguel De Bruycker
General Intelligence and Security Service Cyber Defense, Computer Security Incident Response Capability
Ministry of Defence, Belgium

Isabelle De Vinck
Account Executive
Political Intelligence

Ludwig Decamps
Policy Planning Advisor
North Atlantic Treaty Organisation (NATO) Headquarters (HQ)

Joan Delaney
Public Affairs Consultant

Nicolas Démétriadès
Deputy Armaments Counsellor
Permanent Representation of France to the EU

Georges D'hollander
Director, NATO HQ Consultation, Command & Control Staff (NHQC3S)
North Atlantic Treaty Organisation (NATO) Headquarters (HQ)

Chris Dickson
Journalist - NATO
Agence Europe

Anatoly Didenko
Counsellor
Mission of the Russian Federation to the EU

Shahil Dutta
Stagiaire to MEP Bill Newton Dunn
European Parliament

Nele Eichhorn
Policy Officer, Asylum, Immigration and Borders
European Commission, Directorate General for Justice, Freedom and Security

Nadia El Bennich
Assistant to MEP Bill Newton Dunn
European Parliament

Istvan Erényi
Counsellor, Information Technology
Permanent Representation of Hungary to the EU

Vladimir Forshenev
First Secretary
Mission of the Russian Federation to the EU

Hans-Peter Fuhrer
Representative Armed Forces Planning Staff
Mission of Switzerland to NATO

Sebastiano Fulci
First Counsellor
Delegation of Italy to NATO

Gerard Galler
Policy Officer
European Commission, Directorate General for Information Society & Media

Deyi Gao
Political Counsellor
Mission of China to the EU

Koenraad Gijsbers
Assistant Chief of Staff
NATO - Allied Command Transformation Public Affairs Office (ACT PAO)

Pierre Goetz
Chargé de Mission, Mission Militaire
Permanent Representation of France to the EU

Sarah Greenwood
Government Relations Manager
Symantec Corporation

Michael Grimes
Consultant
Forum Europe

Francesco Guarascio
Section Coordinator
EurActiv.com

Martin Hale
Second Secretary
Permanent Representation of the United Kingdom to the EU

Julian Hale
Freelance

Mattias Hanson
Adviser, Security Policy Department
Ministry of Foreign Affairs, Sweden

Rainer Hellmann
Journalist, European Correspondent
Fuchsbriefe

Jessica Henderson
Senior Manager
Security & Defence Agenda

Diemer Henk
Security Advisory Specialist, Harmful Code Protection Management
IBM Nederland B.V.

Martin Hill
Vice President, Defence
Thales

Thomas Hutin
Director of Information System Marketing
Thales Security Systems Security & Services

Frank H. J. Hye
Senior Advisor
Ministry of Defence, Belgium

Achilleas Kemos
Policy Officer, Internet & Network and Information Security Policies
European Commission, Directorate General for Information Society and Media (Luxembourg)

Micheal Kichmayer
Assistant to M. Weber
European Parliament: Committee on Regional Development

Wolfgang Klasen
Principal Resarch Scientist
Siemens Headquarters

Victor Kochukov
First Counsellor
Mission of the Russian Federation to NATO

Stephane Kolanowski
Legal Advisor
International Committee of the Red Cross (ICRC) EU Liaison Office

Lina Kolesnikova
Advisory Board
Crisis Response Journal Surrey Hills Business Park

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

Justine Korwek
Assistant to James Elles MEP
European Parliament

Dmitry Krasnov
First Secretary
Mission of the Russian Federation to NATO

Christian-Marc Lifländer
Director of the Policy Planning Department & Acting Deputy Undersecretary for Defence Policy
Ministry of Defence, Estonia

Bafana Peter Linda
Police Attaché, 1st Secretary
Embassy of South Africa to the United Kingdom

Edward Lorenzini
Senior Management of Strategy, Strategic Concepts and Initiatives, National & Theater Security Programs
Raytheon

Pier Paolo Lunelli
Deputy Italian Military Representative to EUMC
Permanent Representation of Italy to the EU

Ernest Madzhie
Police Attaché, Counsellor
Embassy of South Africa to the United Kingdom South Africa House

Tiina Maiberg
Second Secretary, Political & Economic Affairs
Embassy of Estonia to Belgium

Jarmo Mäkelä
Bureau Chief
Finnish Broadcasting Company YLE

Pascal Mallet
Journalist
Agence France Presse (AFP)

Mikk Marran
Defence Counsellor
Delegation of Estonia to NATO

Ricardo Martinez De Rituerto
Defence, Foreign Affairs Correspondent
El País

Giacomo Martinotti
Head of European Affairs
Avio

Giles Merritt
Director
Security & Defence Agenda (SDA)

Eliza Miroslawska
Head of Infosec Section
Delegation of Poland to NATO

Dmitry Morozov
First Secretary
Mission of the Russian Federation to NATO

Richard Narich
Conseiller du Président
Altran

Bill Newton Dunn
Vice Chairman
European Parliament, Committee on Budgetary Control

Eugen Nicolae
Expert, Intelligence & International Relations
General Directorate for Intelligence and Internal Protection (DGIPI)

George Vlad Niculescu
Officer, Euro-Atlantic Integration and Partnership Directorate
North Atlantic Treaty Organisation (NATO) Headquarters (HQ)

Jacek Ochman
Assistant of the Polish Military Representative to NATO and the EU
Delegation of Poland to NATO

Adrien Ogée
Assistant
Thales

Reginald Otten
Consultant
Fleishman-Hillard

Serkan Ozdemir
Assistant
Turkish Industrialists' and Businessmen's Association (TUSIAD)

Koya Ozeki
Brussels Correspondent
The Yomiuri Shimbun

Jüri Parbo
Defence Advisor on EDA Matters
Permanent Representation of Estonia to the EU

Petr Pavel
Deputy Military Representative to the EU Military Committee
Permanent Representation of the Czech Republic to the EU

Kees Plas
Head of Security Practice
BT The Netherlands Offices Minerva & Mercurius

Isabelle Roccia
Deputy Editor
SecEUR

Patrick Roccia
Marketing, Critical Systems Branch
Communication et Systèmes (CS)

Jacques Rosiers
Policy Director, Department for Strategic Affairs
Ministry of Defence, Belgium

Piotr Rosolak
Branch Chief
Council of the European Union
General Secretariat of the Council

Geoffroy Roussel
French Navy, Command, Control, Consultations, Communication and Intelligence
North Atlantic Treaty Organisation (NATO) Headquarters (HQ)

Riia Salsa
Spokesperson
Permanent Representation of Estonia to the EU

Leander Schaerlaeckens
Journalist
The Washington Times

Jan-Willem Scheijgrond
Director, Government Affairs
Hewlett Packard

Stephanie Schulze
European Affairs Assistant
European Aeronautic Defence and Space Company (EADS)

Alexander Seger
Head of Economic Crime Division, Directorate General of Human Rights and Legal Affairs

Manos Sfakianakis
Director of the Greek Cyber Crime Unit
Ministry of the Interior and Public Order, Greece

Vadim Shevchenko
Attaché
Embassy of Ukraine to Belgium

Peter Sommer
Visiting Professor, Information Systems Integrity Group
London School of Economics and Political Science

Sander Soone
Representative to the Political and Security Committee (PSC)
Permanent Representation of Estonia to the EU

Viorel Stan
Attaché, INFOSEC Department
Permanent Representation of Romania to the EU

Malle Talvet-Mustonen
Ambassador
Embassy of Estonia to Belgium

Rein Tammsaar
Policy Advisor
Council of the European Union, Policy Planning and Early Warning Unit

Marcin Terlikowski
Analyst
Polish Institute of International Affairs

Oliver Thomassen
Former Project Assistant
Security & Defence Agenda (SDA)

Brooks Tigner
Europe Defence Technology Editor
Jane's International Defence Review
Sentinel House

Raivo-Albert Tilk
Civil-Military Cell
European Union Military Staff (EUMS)

Richard Troy
Policy Officer, Cybercrime and Trafficking in Human Beings
European Commission: Directorate General for Justice, Freedom and Security

Emil Valdelin
Project Manager
Security & Defence Agenda (SDA)

Luc van de Winckel
Corporate Account
Marketing Manager
(EU, NATO, UN, Public Sector)
Hewlett Packard

Ernst van Hoek
Board of Management,
Representative
TNO-Defence Research

David Vasak
Legal Officer, Control of the
Application of Community Legislation
and State Aid/Indirect Taxes
European Commission, Directorate General for Taxation & Customs

Otto Vermeulen
Director - Responsible for the
Security & Technology Practice
PriceWaterhouseCoopers

Wolf-Heinrich von Leipzig
Foreign News Editor
Das Luxemburger Wort

Jonathan Zigrand
Postgraduate Researcher in
International Conflict Analysis
University of Kent Brussels School

About the Security & Defence Agenda

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 Activities:

- Monthly Roundtables and Evening debates
- Press Dinners and Lunches
- International Conferences
- Reporting Groups and special events

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

Permanent Representation of Italy to the EU

Centre for Studies in Security and Diplomacy (University of Birmingham)

Delegation of Romania to NATO

Interested in joining the SDA? Please contact us at Tel: +32 (0)2 737 91 48 Fax: +32 (0)2 736 32 16 Email: info@securitydefenceagenda.org

SECURITY & DEFENCE AGENDA (SDA)

Bibliothèque Solvay, Parc 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