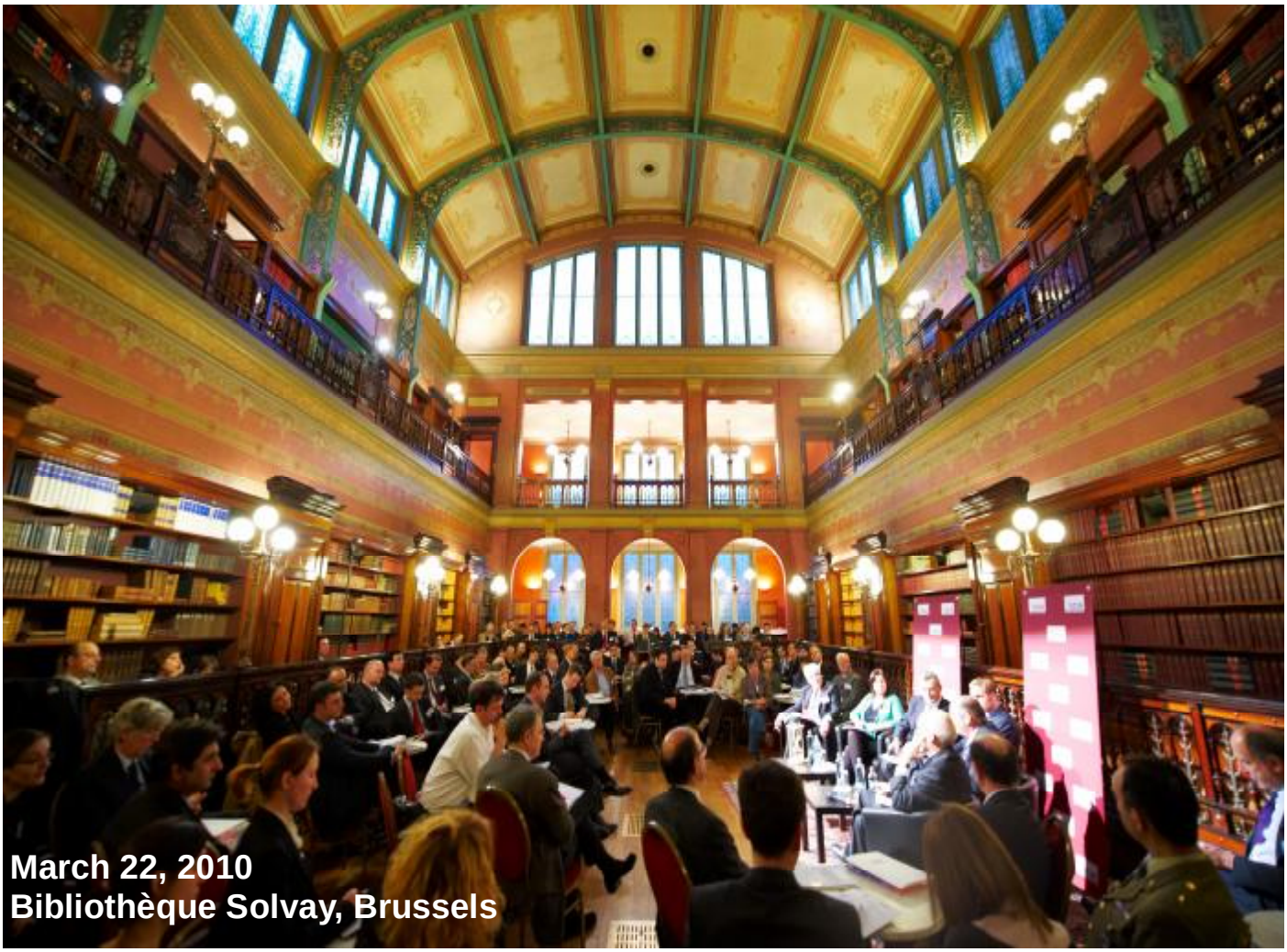
SDA
SECURITY & DEFENCE AGENDA

McAfee®

SDA EVENING DEBATE REPORT

CYBER SECURITY: A TRANSATLANTIC PERSPECTIVE



A ***Security & Defence Agenda*** **Report**
Rapporteur: Paul Ames
Photos: François de Ribeaucourt
Date of publication: April 2010

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

Cyber Security:

A Transatlantic Perspective

Evening Debate – Monday, March 22nd, 2010

Bibliothèque Solvay, 18:00-19:30

On both sides of the Atlantic, policymakers are increasingly concerned that cyber-attacks represent a serious threat. The 2007 "cyberwar" against Estonia has been mirrored in the U.S. by repeated penetrations of secure government and military networks. But how closely are they working together to improve their defences? What steps are being taken by NATO and the EU to coordinate national cyber-defences, and what scope is there for private-public partnerships? In light of the transatlantic tensions created by some counter-terrorism measures, what is the outlook for a common agenda on cyber security?

Programme

17:30 Registration

18:00-19:30 Evening debate

19:30 Cocktail Reception

Speakers

Stewart Baker, Distinguished Visiting Fellow, Center for Strategic and International Studies (CSIS)

Greg Day, Director of Security Strategy, EMEA, McAfee

Ágnes Hankiss, Member of the Committee on Civil Liberties, Justice and Home Affairs, Member of the Subcommittee on Security and Defence, European Parliament

Udo Helmbrecht, Executive Director, European Network and Information Security Agency (ENISA)

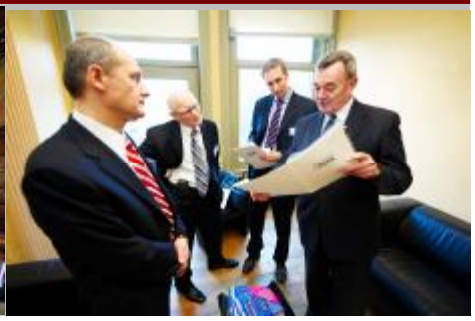
Jamie Shea, Director for Policy & Planning, Private Office of the Secretary General, NATO

Moderator

Giles Merritt, Director, Security & Defence Agenda

Cyber Security: A Transatlantic Perspective





INTRODUCTION

Cyber-warfare is now firmly on the international security agenda.

The dangers range from denial of service attacks that cripple computer networks, to espionage incursions enabling foreign powers to download confidential documents, or the risk that hackers can gain long-distance control over critical infrastructure like power grids, water supply or even weapons systems.

Many in the military now view cyber-space as a new theatre of operations alongside land, sea, air and space, a trend that was underscored by the creation last year of the new U.S. Cyber Command to coordinate America's computer network defences.

Fifty-four percent of IT and security experts taking part in an international survey last year reported suffering large-scale denial of service attacks by a high level adversary such as organized crime, terrorists or nation state.

A similar proportion said they had been subjected to "stealthy infiltration" by high-level hackers and 59 percent said they believed foreign governments had been involved in such attacks or infiltrations, according to the survey by the California-based computer security company McAfee which interviewed 600 experts from 14 countries around the world.

At a debate on the issue organized by the Security Defence Agenda on Monday, 22nd March, senior NATO official **Jamie Shea** said the North Atlantic alliance suffered around 100 cyber incidents everyday.

Georgia's ambassador to NATO **Grigol Mgalobishvili** told the conference his country had come under a cyber attack coordinated with land, air and sea operations during the 2008 war with Russia, which disrupted banking and communications at a crucial time in the conflict.

Other real world examples include the 2007 attacks which swamped Estonian banks, media and government sites during a dispute between the Baltic republic and Russia over the re-location of World War II memorial in Tallinn; and the so-called GhostNet cyber-espionage operation which infiltrated the computers of embassies and government offices of dozens of countries and the Tibetan exile movement close to the Dalai Lama.

Such incidents reflect not only the real and present danger posed by cyber threats but also the difficulty in unearthing the origin of such attacks. Although suspicion fell on Russian sources for the Estonia attacks and Chinese links to GhostNet, no conclusive evidence has been found to connect the incidents to government agencies.

"*We are becoming ever more reliant on technology but we are not necessarily keeping pace with our security* investment"

More than 200 officials from NATO and the EU, politicians, national diplomats, security experts and journalists attended the SDA conference under the theme Cyber Security: a transatlantic perspective.

They heard from McAfee's director of security strategy **Greg Day**; **Stewart Baker**, Distinguished Visiting Fellow at the Center for Strategic and International Studies (CSIS) who co-authored the McAfee survey; Hungarian MEP **Ágnes Hankiss**; **Ronald de Bruin**, head of strategy and public affairs at the European Network and Information Security Agency; and Shea, who serves as director for policy and planning in the private office of NATO's secretary general.

Issues covered ranged from how to define the nature of cyber-warfare and the extent of the risks, to the need for greater coordination both among European nations and between Europe and the United States; and the need


and effectiveness of international "cyber-arms control" agreements.

DEFINING THE THREAT

Baker, former assistant secretary at the U.S. Department of Homeland Security, opened the debate contending that the lines between political cyber attacks and criminal activity have been blurred. For example, he pointed out that the techniques of the GhostNet incursion which seemed to be politically inspired espionage, were quickly imitated by criminal operators to steal from businesses.

The same theme was taken up by Day. "There is actually a dichotomy of which is leading which: is cyber crime leading innovation, that's then being used for cyber warfare, or is cyber warfare leading innovation that's then being picked up for cyber crime?"

Day said MacAfee's research paper last year was an attempt to pin down what exactly the nature of the cyber warfare threat.

"There isn't actually a consistent common definition as to what is cyber warfare." He said they looked at a framework to define it including the sophistication of attacks, the source (i.e.potential of state sponsorship), or the sustainability and consequences of an attack on critical infrastructures and concluded that a lot of the potential targets of even politically motivated cyber attacks were actually in the private sector – such as power grids, banks or water utilities.

"There isn't actually a consistent common definition as to what is cyber warfare"

A key problem is that those private companies are perhaps focused on keeping their business safe from attackers, but seldom looking at the bigger picture of their role in a potential attack on state security. There is a need for financial support and legislation as well as education to improve the private sector's understanding of the threat and define the response, Day said.

"What should we worry about more? That one, very specific targeted attack, or the potential 40 million compromised systems that somebody could either rent part of, or go buy or build for a collaborative attack, whether against a private sector organisation, i.e. something that's perceived to be part of our national infrastructure, or to be used for specific warfare in the future," Day concluded.

"As everybody needs to be connected, everybody makes themselves more vulnerable"

NATO's Jamie Shea pointed out that the ever-growing use of software was creating more and more portals for attackers to gain access. He said the military was increasingly using off-the-shelf software and the Internet.

"As everybody needs to be connected, everybody makes themselves more vulnerable," he warned. However, he recalled that 90 percent of computer penetration continues to be with criminal rather than political or strategic intent.

Much of the political use involves states using "cyber warfare against their own people rather than against others," Shea said, pointing to Iranian government efforts to crack down on the opposition's use of social networks like Twitter to communicate. "Cyber warfare is becoming part of a domestic political struggle, but there is strategic use as well. About 120 countries are now estimated to either have or be in the process of developing offensive cyber attack systems," Shea said. "Strategists are now talking about Cyber as being the 5th domain after space, after sea, after land, after air."

Cyber Security: A Transatlantic Perspective

THE EXTENT OF THE THREAT

Early in the debate, SDA Director **Giles Merritt** asked if future wars would be cyber based "geek-vs.-geek" conflicts fought out by cyber warriors operating keyboards far from traditional frontlines. His comments sparked a sometimes intense discussion on the extent of the cyber threat and whether cyber attacks will replace physical threats or merely be a prelude or sideshow to war in the real world.

Shea asked whether "a cyber attack henceforth would play the same role in initiating hostilities between states that air campaigns played in the 20th century" by softening up adversaries for a military offensive.

"Strategists are still out on this fascinating question as to whether in the future, wars will be wholly won or wholly lost in cyberspace, or whether cyber intelligence will give one side or another an initial advantage, which they may or may not be able to exploit, after which, we'll go back to the usual ways of war fought with weapons that cause physical destruction, rather than simply mass disruption of systems," said the NATO official.

Looking at the range of areas where cyber warfare was already being used, he pointed to the fact that Iraqi insurgents were able to buy a system called SkyGrabber of the internet which briefly enabled them to monitor communications from U.S. drones, until the Pentagon shut them down. He said there was speculation in the defence community that the Israelis successfully planted a bug in Syrian air defence that they were then able to activate, which allowed their air force to attack a nuclear installation under construction a few years ago.

"Cyber attacks are the perfect illustration of asymmetric warfare. It achieves the maximum impact, for the minimum expenditure and the attacker can quickly hide his tracks and even try to blame innocent parties," Shea said. "Entry level is very easy and cheap … a single hacker can paralyse an entire air traffic control system."

He revealed that NATO was the target of about 100 cyber incidents a day. "In a funny way it's a good thing. We're challenged all the time, and we are therefore constantly improving our awareness of the threat and our ability to respond."

In one of the most controversial statements of the evening, Shea sought to put the threat into context, by stressing that the risk from the weapons of mass destruction remains more serious than that from cyber attacks, regardless of its ability to cause mass disruption of the systems on which modern life has come to depend.

"A pre-emptive nuclear strike would be decisive. What we've learned from cyber attacks is that they are very effective for about 36 hours after which, we're on to them … cyber attacks may not have the same kind of impact, at least in military terms as the blitzkrieg bolt from the blue that we've seen earlier," he argued.

"If we had to do without computers altogether in order to be safe from attack, we would go back, not to the Stone Age, which would have been to the consequences of a nuclear war, but back to the 1960s. Life wasn't that bad in the sixties, we got by without computers."

In the question and answer session, **Elly Plooij-Van Gorsel**, an advisor to the Dutch Ministry of Foreign Affairs and former Member of the European Parliament asked Shea how he imagined that the people of 2010

Cyber Security: A Transatlantic Perspective

"Entry level is very easy and cheap… a single hacker can paralyse an entire air traffic control system"

would cope with the lack of computers, mobile phones and other modern communications.

"I think going back to the sixties is not really an option," added Baker.

Shea defended his comments, insisting that his point was that the issue should not be over-hyped. "It's still something that we can deal with quickly. The main disruption, in fact, is likely to be short lived," he said pointing out that even the mass attack on Estonia was brought under control within five days.

"I read in a think tank report the other day… the absurd remark that a cyber attack was the equivalent of an attack by a nuclear weapon; sorry, no! The use of a nuclear weapon would change civilization as we know it … cyber attacks are not at that level."

De Bruin from ENISA said more study was needed to assess the extent of the problem. "How much money do we need to put in there? How big is the problem? It's very difficult to quantify … but we need to prepare ourselves. We have to become more resilient."

Where once the problem was a computer nerd looking for five minutes of fame, the threat is now coming from organizations motivated by criminal or political designs, De Bruin said.

A sobering note was injected into the debate by Georgia's ambassador to NATO Grigol Mgalobishvili who said his country's banks and government web sites were subjected to a cyber attack coordinated with land, sea and air forces during the 2008 war with Russia.

"We have very strong suspicions as to who may be behind it," he said. "This was a critical time when we needed open communications with the outside world … The Georgian case was a good example of how harmful it might be when it is very well coordinated with a military assault. We are now facing a completely new form of warfare."

EUROPE NEEDS TO DO MORE

The focus of the intervention by Hungarian MEP Ágnes Hankiss was the need for Europe to do more to build up cyber defences, including by increasing cooperation both among EU member nations and by working with the United States. It was a theme taken up by several other speakers.

"It is beyond debate that the US and EU must work together in this field and in order to do so more efficiently harmonising our approaches would make sense," said the European People's Party member who sits on the EP's Committee for Civil Liberties, Justice and Home Affairs and the Subcommittee on Security and Defence.

"It is beyond debate that the US and EU must work together in this field and in order to do so more efficiently harmonising our approaches would make sense"

De Bruin said Europe and the United States should plan a common exercise to plan for cyber emergencies and enhance cooperation, building on the Cyber Strom exercises carried out by the US Department of Homeland Security and the EU's debut cyber war games scheduled in November.

"We share the same interests, to protect our economies

and our security," he told the conference. "Security is not a matter of competition, but a matter of cooperation."

Hankiss asserted that the EU's Central European members were more vigilant to the problems of cyber crime due to their recent experience within the Soviet empire. She complained that Russia continues to treat the region as within its sphere of influence and said the EU should make sure it is sufficiently protected from cyber attacks from the East.

Pointing out the use of the internet for recruiting terrorists, Hankiss referred to the link between extremist movements, terrorist acts and the internet. As an example she mentioned her home country, Hungary, where in recent years extreme-right groups have been using the internet for legitimisation purposes. Recruitment and propaganda through anonymous homepages were allegedly financed by the post-communist left.

In the light of the 2007 attacks on Estonia, Hankiss said NATO needed to have a debate on the extend to which a cyber assault on a country's critical infrastructure should be considered an attack under Article 5 of the alliance's founding treaty.

"It is time for discussing and agreeing on a broader term of solidarity which would apply to a cyber attack against a member state's vital civilian or cyber infrastructure," she said.

Pointing to the creation of the Pentagon's Cyber Command last year, Hankiss said the EU should give priority to prevention rather than traction. "We should not run after terrorists," she said.

"It is time for the European Union to reconsider its approach and unify its forces for the sake of the better security of all European citizens, that means Europol, the European Defence Agency, the Commission and all EU bodies dealing with cyber security … a much more focused and coordinated approach is needed." She suggested the EU should launch an "action plan for cyber defence."

Baker recalled that the McAfee survey had indicated serious differences between the levels of engagement in tackling cyber crime by the various EU member states.

"The European Union members ranged from the very top or near the top to the very bottom," he said. The report showed Germany, Spain and Italy near the bottom of the table in terms of measures to improve cyber security, with only India scoring lower. Britain however was one of the best performers behind China and the United states. The range between the EU member states in the survey was greater than the differences between Russia, Brazil, Mexico and India.

"Europe as a whole has yet to arrive at a policy or to implement that policy in a coherent fashion," Baker cautioned.

De Bruin said the first pan-European exercise in November should help improve coordination within the EU. Member states unanimously approved a high level scenario to test the efficiency of cross-border communications links and procedures in times of emergency. In due time the EU and NATO should jointly organize a "transatlantic cyber storm" exercise.

While acknowledging the differences among member nations, De Bruin said there were notable examples of more advanced nations helping others. He cited Hungary's efforts to support the formation of a computer re-

sponse team in Bulgaria as an example.

Journalist **Brooks Tigner**, of Jane's Defence, put the panel on the spot by asking precisely what the transatlantic perspective is. "If it came to a major attack on cyber network it would require a common set of responses … what are the two sides doing?" He also asked if about cooperation between NATO and the European Union, asking if technicians from the two sides are working together "or are you relying on Belgacom?"

"We share the same interests, to protect our economies and our security"

"There is no organised transatlantic response," Baker acknowledged.

"We need to learn from each other. We have to bear in mind that indeed security can lead to competitive advantage on the market, however … we need cooperation," answered De Bruin. "We still have many years to go in order to reach where we want to be."

IS ENOUGH BEING INVESTED IN CYBER DEFENCE?

Merritt put the question to Greg Day of whether advanced countries spend enough on cyber-defences.

In reply the McAfee director said it was important to ascertain if the ever increasing number of detected incidents was a sign that the situation is getting worse, or if it showed that companies like his were getting better at detecting them.

"In my view more is better, we're doing the right thing," was his reply.

Referring to the McAfee report he said most of those surveyed believed that they had adequate levels of security. However, he warned that about a quarter of them had dropped their security investment by 15 percent or more in response to the economic crisis. He warned that there is a danger that more and more companies were investing in technology to reduce labour costs, but at the same time were cutting security budgets.

"We are becoming more reliant on technology but we're not necessarily keeping pace with our security investments," Day said.

The survey showed that the financial sector, which is heavily reliant on technology, comes under the most consistent attacks and as such has the highest level of investment to tackle the problem. In contrast companies in the water or sewage systems may consider themselves at lower risk and have invested less in protection. However they could be vulnerable to a cyber attack that could have devastating effects at a regional or national level.

"We have to understand the risk, not only to our own organizations but also in terms in terms of what does that mean to our nation."

To give an idea of the scale of the problem, he said McAfee last year found over 40 million public systems compromised by long distance takeover that turned them into zombies that can be used to launch attacks by their hidden controllers. Over 6,000 new threats are uncovered every day he said.

Jamie Shea said NATO should perhaps contemplate a move away from the Internet to move back to private enclosed systems with built-in firewalls.

HOW CAN THE EU AND NATO BUILD UP DETERRENCE AND COUNTER-ATTACK CAPACITY?

In nuclear or conventional conflict, the possibility of retaliation could act as a deterrence, but in the cyber world, it's difficult to even know who the enemy is, Shea said.

"A real problem is to rethink deterrence," he said. He questioned if the conventional response of blocking attacks, detecting the culprit and seeking diplomatic sanctions are sufficient. "Do we have to have some kind of retaliatory cyber-attack policy? Who initiates that? Do we have to have a war powers resolution from the US Congress for a government to formally initiate cyber retaliation? Do we leave that in the hands of the defence establishment to decide on alone? Can we retaliate only with equivalent cyber measures or can we use other types of military measures?"

Other issues to be resolved are when a civilian police response is more appropriate and when the military needs to get involved. Then, there is what Shea called the "Thomas Becket syndrome" where a state doesn't actually initiate an attack, but tacitly gives a private operator the go-ahead.

"In that scenario is a state legally responsible for the actions of its citizens who think they are operating on its behalf?" he asked.

"This is an area where the law … is extremely murky," he concluded, suggesting that the SDA should bring experts together to look at a possible framework.

David Fouquet, director of the Asia-Europe project, asked about the role of preventive diplomacy with the idea of launching multilateral consultations or international cyber arms control agreements. The idea was given short shrift by Baker.

"We shouldn't do any of those things because we don't have any assured responses that scare anyone. We haven't promised a kinetic response and we wouldn't know where to send the cruise missiles if we were to promise one," he argued. "It would turn out to be a unilateral disarmament in a situation where we are virtually disarmed today."

"This is an area where the law… is extremely murky"

Greg Day pointed out that the Council of Europe already has a cyber crime convention but to date still very few nations have signed up to it.

Shea however expressed interest in the idea of international conventions, perhaps to commit nations to allow Interpol investigations on their territories if they are suspected of being used as the base for cyber attacks, or an agreement not to target civilian targets such as hospitals or water systems. "There are far more questions than answers in this area," he acknowledged.

List of Participants

Paul Ames
Freelance Journalist

Pascale Andréani
Ambassador
Delegation of France to NATO

Darko Arabadzic
Second Secretary
Mission of Croatia to the EU

Frank Asbeck
Principal Adviser, Human Resources and Security
European Commission
Secretariat General

Maria Åsenius
Head of Cabinet
European Commission
Cabinet of EU Commissioner for Home Affairs
Cecilia Malmström

Paul Baes
Former Official
Council of the European Union
Directorate General for External Economic and Politico-Military Affairs

Stewart Baker
Distinguished Visiting Fellow
Center for Strategic and International Studies (CSIS)

Hanka Balajkova
Trainee
European Commission
Secretariat General

Mira Banacka
Second Secretary
Delegation of Slovakia to NATO

Mohamed-Raja'l Barakat
Expert

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

Robert Bell
Senior Vice President European Business
Science Applications International Corporation (SAIC)

Emanuela Bellan
Head of Unit, Crisis Management Unit, SG/B/3
European Commission
Secretariat General

Eva Bengtsson
Security Trainer, Security Directorate
European Commission
Directorate General for Justice, Freedom and Security

Esmerelda Berghen
Candidate Professional Officer - Junior Lieutenant
Royal Military Academy, Belgium

Ivan Bizjak
Director General
Council of the European Union
Directorate General for Justice & Home Affairs

Antoaneta Boeva
Gender Balance and Diversity Officer
North Atlantic Treaty Organisation (NATO)

Christian Boone
Member
Association for Intercultural Education

List of Participants

Jiri Burianek
Director, Industry, Research & Telecommunications
Council of the European Union
Directorate General for Internal Market, Competitiveness, Industry, Research

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

Myriam Buyse
Secretary
Association des Anciens des Communautés européennes (AIACE)

Leo Buzzerio
Assistant Army Attache
Embassy of the United States of America to Belgium

Geert Cami
Co-Founder & Director
Security & Defence Agenda (SDA)

Giuseppe Cantalini
INFOSEC Officer
North Atlantic Treaty Organisation (NATO)

Daria Catalui
MA Student, Security Studies
University of Bucharest

Olivier Chassagne
Team Leader, EGNOS, Galileo Exploitation
European Commission
Directorate General for Enterprise and Industry

Gintaras Čiurlionis
Minister Counsellor
Permanent Representation of Lithuania to the EU

Lefteris Coroyannakis
Executive
Brunswick Group

Robert Cox
Trustee
Friends of Europe
Les Amis de l'Europe

Claudia Cruz
Intern
United Nations Regional Information Center for Western Europe (UNRIC)

Atu Darko
Public Affairs Officer
North Atlantic Treaty Organisation (NATO)

Stanislav Daskalov
Head of Brussels Liaison Office
Regional Cooperation Council
Brussels Liaison Office

Greg Day
Director of Security Strategy, EMEA
McAfee
Corporate Headquarters

Ronald De Bruin
Head of Strategy and Public Affairs department
European Network and Information Security Agency (ENISA)

François de Ribaucourt
Photographer

Joan Delaney
Independent Consultant

Nora Delaney
APCO Worldwide Brussels Office

List of Participants

Polydoros Demetriades
Principal Administrator
European Commission
Directorate General for Education and Culture

Emmanuel Devigne
Deputy COS
Permanent Representation of France to the EU

Anatoly Didenko
Counsellor, Home Affairs
Mission of the Russian Federation to the EU

Eleni Dima
Public Affairs Office Intern
North Atlantic Treaty Organisation (NATO)

David Henry Doyle
Communications and Policy Officer
Security & Defence Agenda (SDA)

Philip Eder-Levacher
Senior Account Executive
Fleishman-Hillard

Fredrik Ekfeldt
Principle Administrator
Council of the European Union
EU Joint Situation Centre

Abdelghafour El Otmani
Student
Université Catholique de Louvain (UCL)

Carlos Enriquez
Assistant Defence Counsellor
Delegation of Spain to NATO

Aksel Ethembabaoglu
Policy Analyst
The Hague Centre for Strategic Studies

Alessandra Falcinelli
EU official, DG information Society and Media
European Commission

John Fay
Commercial Officer
Mission of the United States of America to the EU

Rafael Fernandez-Pita y Gonzalez
Deputy Director General
Council of the European Union
Directorate General for Justice & Home Affairs

David Fouquet
Director, Editor
The Asia-Europe Project

Octavia Frota
Senior Advisor

Elena-Dana Frunzeti
Defence Counsellor, Head of Defence Section
Delegation of Romania to NATO

Marie Fuchs-Drapier
Crisis Management Unit
European Commission
Secretariat General

Hans-Peter Fuhrer
Staff Officer, Military Section
Mission of Switzerland to NATO

Konrad Fuhrmann
Project Manager
European Commission
Directorate General for Translation

Yoshinori Fukushima
Senior European Correspondent & Bureau Chief
Mainichi Shimbun Brussels Office

List of Participants

George-Wilhelm Gallhofer
Austrian delegate to the COTRA working group
Permanent Representation of Austria to the EU

Thomas Gann
Vice President Government Relations
McAfee

Bill Giles
Director General Europe
BAE Systems

Sarah Greenwood
European Policy Manager
Google

Kestutis Gruodis
Analyst, Intelligence Directorate
European Union Military Staff (EUMS)

Karolina Grzyb
Unit A2 – Information, Communication
European Commission
Directorate General for Enlargement

Ágnes Hankiss
Vice-Chairwoman
European Parliament
Sub-Committee on Security and Defence

Udo Helmbrecht
Executive Director
European Network and Information Security Agency (ENISA)

Mathieu Hoeberigs
Principal Administrator, Tourism
European Commission
Directorate General for Enterprise and Industry

Henna Hopia
Project Manager
Security & Defence Agenda (SDA)

Gianfranco Incarnato
Deputy Permanent Representative
Delegation of Italy to NATO

Jan Jacek
Official
Permanent Representation of the Czech Republic to the EU

Jens-Henrik Jeppesen
Director, Government Affairs
Dell Computers Belgium

David Johnson
Governance and Security
European Commission
Directorate General for Development and Relations with ACP States

Jeroen Kelders
Candidate Professional Officer - Junior Lieutenant
Royal Military Academy, Belgium

Michalis Ketselidis
Crisis Management Unit
European Commission
Secretariat General

Radek Khol
Civilian Crisis Management
Council of the European Union
General Secretariat

Galina Khorkova
Researcher
University of Kent
Brussels School of International Studies

List of Participants

Kristian Dambo Knudsen
Project Assistant
Zealand Denmark EU Office

Dmitry Kosarev
Correspondent in Belgium
Rossiyskaya Gazeta

Boris Kremenetskyi
Counsellor for ESDP
Mission of Ukraine to the EU

Anton La Guardia
Security and Defence Correspondent, London
The Economist

Jean Labrique
Secretary General
Western Defense Studies Institute

Yves Lagoude
European Affairs Director, Thales Security Solutions and Services
Thales

Raphaël Lallemant
ICT Chief
Coordination Unit for Threat Analysis (CUTA)

Lionel Lechien
Euro-Atlantic Association of Belgium

Thomas Lenschen
Project Officer CIS
European Defence Agency (EDA)
Armaments Directorate

Hillar Leoste
Security of Sensitive Information and Communication Systems
Council of the European Union
Directorate General for Personnel and Administration

Lauri Lepik
Deputy Permanent Representative
Delegation of Estonia to NATO

Ruben Lombaert
Policy Officer
European Commission
Directorate General for Justice, Freedom and Security

Pablo Lopez-Alvarez
Senior Associate
FD Blueprint

Valeria Lunadei
NAGSMO BOD Head Permanent Secretariat
North Atlantic Treaty Organisation (NATO)

James Kevin MacGoris
Head of Communications
Security & Defence Agenda (SDA)

Utimia Madaleno
R&T Assistant Director
European Defence Agency (EDA)
Armaments Directorate

Guido Maene
EBNO
Ministry of Defence, Belgium
Department Strategy Defence Transformation Advice

Ruslan Magomedov
Diplomat
Embassy of Russia to Belgium

Pascal Mallet
NATO and EU Defence Correspondent
Agence France Presse (AFP)

List of Participants

Mifundu Mamaku
Member
Forum Interrégional des Femmes Congolaises (FIREFEC)

Maria Mas
Isdefe

Pauline Massart
Senior Manager
Security & Defence Agenda (SDA)

Olivier Masseret
EU Affairs Manager / Key account Manager EU-NATO
European Aeronautic Defence and Space Company (EADS)

Zurab Matcharadze
European Correspondent
Resonance Daily Newspaper

Isto Mattila
Policy Officer
European Commission
Directorate General for Fisheries & Maritime Affairs

Michael McLaughlin
Air Attaché
Embassy of the United States of America to Belgium

Natalia Melnyk
Third Secretary
Mission of Ukraine to NATO

Julian Memetaj
Student

Giles Merritt
Director
Security & Defence Agenda (SDA)

Olivier Mesotten
Analyst
Coordination Unit for Threat Analysis (CUTA)

Grigol Mgaloblishvili
Ambassador
Mission of Georgia to NATO

Harris Minas
Intelligence Analyst
Sandstone

Vladimir Minkevich
Defence Attaché
Embassy of Russia to Belgium

Tomeu Mir
Assistant to Teresa Riera Madurell
European Parliament

Eliza Mirosławska
Counsellor, INFOSEC Branch
Delegation of Poland to NATO

Annalisa Monaco
Director EU and NATO Relations
The Boeing Company

Marco Moreschini
Seconded National Expert, Adviser Trainer, Security Training & Awareness Team, Security Directorate- Inspection and Advisory
European Commission
Directorate General Human Resources and Security

List of Participants

Levente Nagy
Policy Advisor to MEP Ágnes Hankiss
European Parliament

Antonio Nogueras
Head Agency Security Office
EUROCONTROL

Carmen Oprea
Regulatory and Policy Associate, EU Liaison Office
European Federation of Energy Traders (EFET)

Reginald Otten
Account Director
Fleishman-Hillard

Christos Papazaris
Security Intelligence Analyst
European Commission
Directorate General Human Resources and Security

Tornike Parulava
Counsellor
Mission of Georgia to NATO

Anabela Pereira
Coordinator for Internal Communication
European Commission
Directorate General for Translation

Isabelle Pernot du Breuil
Associate
Direction Internationale Associées

Iulia Platona
Development Policy Task Manager
Network Development Policy EUGAD

Elly Plooij-Van Gorsel
Director
Elly Plooij Consultancy

Romain Poly
European Affairs Manager - EU & NATO Affairs Department
Thales

Constantinos Prevelakis
Independent consultant

Rebecca Pugh
Co-desk, USA, Canada
European Commission
Directorate General for External Relations

Elizabeth Quiring
Diplomat
Embassy of the United States of America to Belgium

Timm Rentrop
Legal Officer, EU Labour Law
European Commission
Directorate General for Employment, Social Affairs and Equal Opportunities

Kyriakos Revelas
Senior Security Policy Analyst, Security Policy Unit
European Commission
Directorate General for External Relations

Nélia Ribeiro
Intern
United Nations Regional Information Center for Western Europe (UNRIC)

Isabelle Roccia
Senior Consultant
Schuman Associates

Antonio Leao Rocha
Counsellor
Permanent Representation of Portugal to the EU

List of Participants

Patricia Rodriguez
Project Manager
Fundacion Comunidad Valenciana-Region Europea

Albena Rousseva
DG E IV - Transatlantic Relations
Council of the European Union

Paolo Salieri
Principal Policy Officer
European Commission
Directorate General for Enterprise and Industry

Bojan Savic
Lecturer, PhD Candidate
University of Kent
Brussels School of International Studies

Donald Scargill
Director
Information2Intelligence

Teri Schultz
Freelance Journalist
National Public Radio (NPR)

Frederik Schumann
Consultant
CEIS European Office

Jamie Shea
Director for Policy Planning, Private Office of the Secretary General
North Atlantic Treaty Organisation (NATO)
NATO Headquarters (HQ)

Vladimir Silhan
Defence Advisor
Permanent Representation of the Czech Republic to the EU

Bart Smedts
Fellow researcher, Royal High Institute for Defence
Ministry of Defence, Belgium

Philip Springuel
Director
PAS Project Management

Chris Stace
Action Officer, CIS Directorate
Council of the European Union
Directorate General for External Economic and Politico-Military Affairs

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

Willy Stevens
Honorary Ambassador
Ministry of Foreign Affairs, Belgium

Andreas Strauss
Counsellor, Military Affairs
Mission of Austria to NATO

Anna Szatkowska
Researcher
Open Europe Brussels

György Tatar
Head of Task Force on Horizontal Security Issues
Council of the European Union
General Secretariat

Christof Tatschl
Chief of Staff and Military Counselor
Mission of Austria to NATO

Olivia ten Horn
Project Assistant
Security & Defence Agenda (SDA)
La Bibliothèque Solvay

Zoran Thaler
Member
European Parliament
Committee on Foreign Affairs

List of Participants

Damian Thwaites
First Secretary (Defence Planning & Capabilities)
Delegation of the United Kingdom to NATO

Irina Tica-Diaconu
Second Secretary
Permanent Representation of Romania to the EU

Brooks Tigner
Editor and Chief Policy Analyst
SecEUR

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

Janos Tisovszky
Deputy Director
United Nations Regional Information Center for Western Europe (UNRIC)

Carlos Torralba
Subject matter expert
North Atlantic Treaty Organisation (NATO)
NATO Headquarters (HQ)

Antonio Torres
Head of International Business Development
Isdefe

Johann Trummer
National Armaments Director Representative
Mission of Austria to NATO

Deniz Turgay
Intern
Turkish Industry and Business Association (TUSIAD)

Luc van de Winckel
Senior Manager, Business Development
Lockheed Martin Global

Iveta Vanurova
Security Officer
European Commission
Directorate General Human Resources and Security

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

Jelena Vasic
MA Student
University of Kent
Brussels School of International Studies

Liana Vasilache
Assistant
Council of the European Union

Yaroslav Vasilyev
First Secretary
Embassy of Belarus to Belgium

Sal Viveros
Senior Director, Worldwide Enterprise PR
McAfee

Christina von Westernhagen
Director, EU Government Affairs and Public Policy
The Dow Chemical Company Europe

Kostyantyn Voytovsky
Counsellor, Defence Intelligence
Mission of Ukraine to NATO

Anja Vvedenskaia
Brussels Corresponent
Novoye Russkoye Slovo (NRS com)
NRS Publishing Corp

List of Participants

Philip Wiese
Assistant Policy Officer, DG Information Society
European Commission
Secretariat General

Andrea Cornelia Windhab
Brussels Representative
Eurisc Foundation

Erik Windmar
Personal Assistant to the Commissioner, External Relations, Research, Innovation & Science, Defence & Space
European Commission
Cabinet of EU Commissioner for Home Affairs
Cecilia Malmström

Xiaoguang Yang
Second Secretary
Mission of the People's Republic of China to the EU

Julia Zalutskaja
Assistant to the Secretary for External Relations
European People's Party (EPP)

Luca Zampaglione
Official
North Atlantic Treaty Organisation (NATO)
NATO Headquarters (HQ)

About the SDA

SDA
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
- Discussion Papers and special events

SDA
SECURITY & DEFENCE AGENDA

The Security & Defence Agenda would like to thank its members and partners for their support.

NATO OTAN
LOCKHEED MARTIN
Konrad Adenauer Stiftung
IBM
MINISTÈRE DE LA DÉFENSE
EADS
hp invent
Raytheon
TEXTRON Systems
BOEING
symantec.
ASD
SAIC
Honeywell
SES
THALES
United Technologies
Avio
McAfee
DCNS
MBDA MISSILE SYSTEMS
BAE SYSTEMS
SAAB
PRICEWATERHOUSECOOPERS
FINMECCANICA
CSIS
EDA
TNO
THE ATLANTIC COUNCIL OF THE UNITED STATES
GCSP
Hanns Seidel Foundation
sipri
FONDATION ROBERT SCHUMAN
ISIS europe
Centre for Studies in Security and Diplomacy (University of
eu2006.fi
ISN Run by CSS
RUSI
CESS Centre for European Security Studies
World Security Network
faes
EGMONT
CSSM Centre for Security Sector Management
DCAF
SECURITY EUROPE

The SDA gratefully acknowledges the generous support from the following

France
Romania
United States
Russia
Netherlands
Turkey
Czech Republic
Italy
Finland
Belgium

Interested in joining the SDA? Please contact us at Tel: +32 (0)2 739 1582
Fax: +32 (0)2 736 3216 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
www.securitydefenceagenda.org