

SDA Report

# Getting in step: Coordinating national responses to changing security threats

24 February, 2011  
Bibliothèque Solvay, Brussels



A *Security & Defence Agenda* Report

Rapporteur: Jonathan Dowdall

Photos: Philippe Molitor

Date of publication: March 2011

**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](mailto:info@securitydefenceagenda.org) / W: [www.securitydefenceagenda.org](http://www.securitydefenceagenda.org)

Twitter: <http://twitter.com/secdefagenda>

CONTENTS

Speakers and moderator 2

Introduction 3

Emerging security challenges 3

The cyber domain 5

The importance of coordinating information sharing 6

Getting in step — conclusions 8

List of participants 10

SDA Advisory Board 16

About IBM 19

About the SDA 20

The views expressed in this report by speakers are personal opinions and not necessarily the views of the organisation they represent, nor of the Security & Defence Agenda, its members or partners.

Reproduction in whole or in part is permitted, providing that full attribution is made to the Security & Defence Agenda and to the source(s) in question, and provided that any such reproduction, whether in full or in part, is not sold unless incorporated in other works.

## Evening debate

Thursday 24 February 2011  
Bibliothèque Solvay, Brussels

NATO's new Emerging Security Challenges division highlights the need to monitor and prepare for non-traditional security challenges like cybersecurity, energy security and terrorism. Will this new structure give NATO the teeth it needs to properly coordinate national policies in this area? What hurdles remain, particularly in the area of intelligence-sharing? How is the EU reacting to these new concerns, and are their mechanisms likely to compliment or compete with NATO's?

### Speakers



**Harriet Pearson**  
*Vice President*  
Security Counsel & Chief Privacy Officer  
IBM



**Richard Wright**  
*Director*  
Conflict Prevention & Security Policy  
European External Action Service (EEAS)



**Jamie Shea**  
*Deputy Assistant Secretary General*  
NATO Emerging Security  
Challenges Division

**Ivo Veenkamp**  
*Director for Policy and Strategy*  
National Coordinator for Counterterrorism  
The Netherlands (NCTB)

### Moderator



**Giles Merritt**  
*Director*  
Security & Defence Agenda

# Getting in step: Coordinating national responses to changing security threats



## Introduction

From the policies of the European External Action Service to NATO's new Emerging Security Challenges Division, in the past year a great deal of attention has moved to the idea of "new" or "emerging" security challenges. Faced with complex problems such as cybersecurity, critical infrastructure protection and terrorism, European governments are increasingly called upon to "get in step", and coordinate fragmented national initiatives.

Against this backdrop, a panel of high-level experts with varied national, international and industry backgrounds gave participants insights into the challenges of dealing with emerging threats. The evening's discussion focused on a number of themes, from information-sharing to the new

---

*"NATO is using this as an opportunity to reassess what we've been doing in certain areas that we have been grappling with for some time already... and asking ourselves if we've really been producing what we hoped".*

---

characteristics of the cyber-domain. Yet ultimately, participants agreed that it was not the "newness" of such threats that was hampering Europe's response. Rather, as Richard Wright, Director for Conflict Prevention and Security Policy in the European

External Action Service (EEAS) stated, "getting in step must include the development of a closer commonality of approaches" between diverse agencies and nations.

## Emerging security challenges

The speakers began by outlining the daunting array of new security threats. The broad scope of this agenda was aptly summarised by Jamie Shea, Deputy Assistant Secretary General of NATO's Emerging Security Challenges Division. In a rapid break-down of numerous policy fields, Shea explained how this new division had been created to address issues of counter-terrorism, critical infrastructure protection, cybersecurity and non-proliferation. These challenges may be rooted in new technologies such as cyber-attacks, or forms of political violence such as terrorism. Regardless, what set them apart was their rapid emergence in the last decade as growing threats to European member states.

Shea admitted that some of these threats were not completely new to the Alliance. However, "NATO is using this as an opportunity to reassess what we've been doing in certain areas that we have been grappling with for some time already... and asking ourselves if we've really been producing what we



## Getting in step: Coordinating national responses to changing security threats



---

*“Security is by definition cross-sectoral and cross-border, so you have to act externally to achieve internal security, and vice versa”.*

---

hoped.” Overall, Shea was confident that a re-focus on these new challenges could support attempts “to pull in coherence and results where they did not exist before”.

Wright agreed with this summary of the threat environment, but through the prism of the EEAS added an external dimension to these themes. “Security is by definition cross-sectoral and cross-border, so you have to act externally to achieve internal security, and vice versa”, he explained. The result of this “need to promote coherence and complement it between internal and external actions”, was that “you can’t deal with these things by looking at only one aspect”.

The obvious conclusion was the need for a “comprehensive approach” to deal with new security challenges. Serious state security issues such as terrorism or non-proliferation need to be addressed through many different disciplines. These include contrasting competencies such as law enforcement, criminal justice, border management and resilience to disasters. Clearly, such an agenda

calls upon the EU and its members to pursue “trans-national and regional approaches”, and to “carefully reflect on our instruments and means” in different areas of security, he concluded.

This merging of previously separate security fields was picked up by Ivo Veenkamp, Director for Policy and Strategy with the National Co-ordinator for Counterterrorism of the Netherlands. Reflecting on practices within his national organisation, he asserted the need for “open-mindedness” when assessing new security challenges. This changing threat environment can leave nations unprepared or surprised by developments in fields such as terrorism or critical infrastructure protection. “Don’t only look at things that may pose a threat today, but look at new developments which may become a risk in the future”, he cautioned.

To achieve this level of foresight, it is important to “gather, analyse and question the information available”, he continued. Otherwise, the focus on a comprehensive approach will be wasted through faulty information. Only a wholly accurate assessment can forestall a security failing. Finally, the importance of closely connecting analysis, policy and implementation as well as keeping your team small, proactive and forward thinking were the Dutch expert’s best pieces of advice for dealing with inherently unpredictable emerging security threats.

## Getting in step: Coordinating national responses to changing security threats



### The cyber domain

The unpredictable nature of new security challenges is nowhere more evident than in the rapidly changing field of cybersecurity, and coordination in the cyber domain was a major theme of the debate. Harriet Pearson, Vice President, Security Counsel & Chief Privacy Officer for IBM, explained that the proliferation of network-capable technologies had given cybersecurity actors a host of “interesting and strategic challenges”.

One such problem was what technical experts have dubbed “de-perimeterisation”, she explained. “In the security field, the traditional concept was that you draw a perimeter and you protect the perimeter; and that would suffice in that trusted insiders could function”. However in the new technology environment, “the perimeter has morphed, it has changed”, to include portable and wireless technologies, critical infrastructure electronics and even domestic transport. The result is a “landscape that is justifiably looked at as a threat landscape”.

Faced with this new landscape, Shea acknowledged that the cyber domain was “one of the major

priority areas for NATO, because we may have to catch up with the speed of developments”. One part of this institutional focus would be to better conceptualise aspects of cybersecurity. Member states need “a beefed up cyber concept, with a broader ambition that goes beyond NATO’s own systems”, he asserted. For NATO’s deterrent function, it was important to understand how “these new concepts of defence fit into existing structures”. Only when members had a clear set of “rules of the road” for cyber-conduct could threatening behaviour be properly gauged and dealt with, he concluded.

Harriet Pearson agreed that collaborative standards of national conduct could aid cybersecurity and infrastructure protection, by guiding the development of good security practices. “Governments of all sizes and all scopes should not underestimate the power they have to lead by example and truly pull behaviours along in the private sector”, she affirmed. By encouraging coordination between national regulations on cybersecurity, Europe could seek true “security by design” in their complex systems.

---

*“Governments of all sizes and all scopes should not underestimate the power they have to lead by example and truly pull behaviours along in the private sector”.*

---

## Getting in step: Coordinating national responses to changing security threats



Yet cybersecurity is not just about networks, it is also about the integrity of the hardware and software that Europe relies on. Frans Picavet, Global NCO Ambassador for IBM Belgium raised this point, asking if the fact that much software is now “open-source” (written and donated by online users) could compromise critical systems. In response, Pearson was adamant that open-source software as such, was not a significant security threat. Due to the large number of individuals involved in coding, “there’s an inherent security that comes along with more ‘eyes on the code’”, she explained. As long as you had a professional level of scrutiny on new programming, the danger is low.

However, the potential for electronics manufactured abroad to be infected prior to delivery into key European systems did raise some concern, with Shea asking “how do you actually ensure the equipment you are buying doesn’t contain viruses at the production stage?” Pearson agreed that reliability and trust in industrial products was a key aspect of cybersecurity collaboration. She then elaborated some possible solutions, including the Trusted Technology Forum, a commercial initiative intended to create the “framework for global standards and best practices for how to build technology with integrity” in manufacturing electronics.

The conclusion was clearly that dealing with the emerging security challenges of the cyber domain would require “a global collaboration, both private and public, that will add to existing cyber criteria for security”.

### The importance of coordinating information sharing

An important facet of coordinating responses to emerging security threats is the need to share information between detached institutions and agencies. This was a challenge elaborated by many participants. Wright was a strong proponent, saying that “when different institutions are dealing with these issues, clearly, we need to share information”. Elaborating on the EU’s relationship with NATO, he added that “we informally tell each other what we are doing in new areas” on a regular basis. With these major institutions sharing a majority of members and resources, it is obviously “useful and important to not tread on each other’s toes”.

Shea agreed, and in response to a question from the floor about risk assessment, explained the practical ways that NATO and the EU were collaborating to create a broader intelligence picture for their members. NATO’s BICES intelligence distribution



## Getting in step: Coordinating national responses to changing security threats



centre was one example, which allows “more and more risk assessment and intelligence information” to be collated and made available “24/7” for counter-terrorism or operational purposes. “The EU is plugged in to this system”, Shea asserted, which improved the flow of information amongst complementary missions both in Europe and beyond.

Veenkamp went further, arguing that the quality of information was also improved

---

*“A big threat for a national government is that you lose contact with what is happening on the ground”.*

---

by such cooperation. “When you look at counter-terrorism, you have to be able to connect the local with the national with the international”, he explained. Faced with this challenge, “a big threat for a national government is that you lose contact with what is happening on the ground”. Sharing professional opinions and perspectives between institutions can help individual actors develop a more accurate picture of events. “Don’t only look for people who have the same background as yourself”, he concluded.

Whilst sharing information is clearly important for predicting future vulnerabilities in the long term, some questioned the effectiveness of these principles in fast-paced emergencies. Alexander von Lingen, Chair of EquipEurope picked up the point.

“Coordination is very useful in the centre, but I wonder, how can coordination work in the field, where you cannot sit and discuss, but decisions have to be taken very fast?”, he asked.

Pearson agreed that an important aspect of the new information sharing environment was the growing responsibility for front-line staff to process intelligence. “Horizontal power structures are increasingly important and are supplementing, maybe even re-orientating, previously vertically structured organisations”, she explained. Information must be “pushed out into the periphery, to the front-lines”, if it is to be of use.

Veenkamp also believed that “horizontal information relationships are becoming more important” when dealing with critical decisions on the ground. To coordinate and execute decisions based on shared information, “one of the crucial competencies is that they [staff] are able to deal with dilemmas”, he continued. “There is no such thing as a simple decision”, and operatives dealing with emerging security challenges are increasingly called upon to show good judgement when receiving information.

## Getting in step: Coordinating national responses to changing security threats



Another problem may be the availability of too much information, Shea cautioned. "Having all of this information is great, it can also save lives, but we need to learn how to process it all effectively". The risk of information "overload", especially in a digitalised information environment was "one of the biggest challenges now" for coordinating action, he asserted. From intelligence processing to coordinating operational responses, "having spent 20 years gathering more data, the challenge will be to rein it in [...] and start to be more discerning in how we manage information".

The sharing of information between agencies prompted a question about data security from Elisa Oezbek, consultant, ESC-Counterterrorism Section at NATO. Referencing the Wikileaks scandal, she asked "if more people know more, will that become a bigger security threat to information?" Veenkamp agreed that data protection breaches such as Wikileaks raised serious questions about the volume of information that is passed freely between security actors. "It is a strange idea that all information should be available to everyone – of course not", he retorted. Pearson also agreed that there was a need to balance access and "the need to know". Rather than clamping down on information exchange, it was more important that

partners agreed in advance "what do we need to share, who needs to see it, what are the access controls?"

It was concluded that dealing with emerging security challenges would require careful consideration of the volume, quality and security of information exchanged. Regardless, sharing such information was necessary, and required members to consider "how to preserve the benefits of the open system in an information security context", said Jamie Shea.

### Getting in step - conclusions

Threats such as terrorism, cybersecurity and WMD proliferation call for transnational and cross-border solutions. Throughout the evening's discussion, participants advocated a free exchange of information and expertise between different security actors to better meet these challenges.

Yet in reaching this conclusion, it was striking how many of the proposed solutions to new threats were rooted in very old problems of institutional and bureaucratic impediments to coordination.

## Getting in step: Coordinating national responses to changing security threats



As Shea pointed out, “everybody is well aware of the state of the EU-NATO relationship”, and its failings. His call to “work together pragmatically where we can” has been a common one for these two institutions. Equally, Wright lamented how different departments within the European Commission lacked a common approach. “The financial instruments are not joined up, and have different legal bases”, he explained. The EU’s institutions are themselves lacking coordination. Veenkamp also stressed the need to work hard to “foster and connect your own organisation on many levels”.

These problems are recognizable ones. European nations have historically wrestled with cooperation and coordination in many security fields. So whilst emerging threats may stimulate discussion about new environments or dangers, the new comprehensive solutions proposed by the panel will require some traditional solutions. As Wright stated, “getting in step must include the development of a closer commonality of approaches”.

## List of participants

Gerhard Ahlbrecht  
*Secretary General*  
European Organisation of Military Associations  
(EUROMIL)

Keith Anderson  
*Office Director*  
United States Air Force, Office of General Counsel

Gintautas Baranauskas  
*Administrator*  
Council of the European Union

Giuseppe Belardetti  
*Program Director*  
Atlantic Treaty Association (ATA)

Piotr Blachowski  
*First Counsellor, Justice & Home Affairs*  
Permanent Representation of Poland to the EU

Sergey Bludnov  
*Third Secretary*  
Permanent Mission of the  
Russian Federation to NATO

Pawel Bodnar  
*Security Expert*  
Council of the European Union

Adrian Bourceanu  
*Second Secretary*  
Permanent Representation of Romania to the EU

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

Guadalupe Casas  
*Independent Journalist*

Frederic Chedham  
*Director*  
CLA Consulting

Jacques Cipriano  
*Vice President, European Affairs*  
Safran Group

Michèle Coninx  
*Vice-President*  
The European Union's Judicial Cooperation  
Unit (EUROJUST)

Andrew Cox  
*Vice President, Business Development*  
*EU and NATO*  
Lockheed Martin Global, Inc.

Robert Cox  
*Trustee*  
Friends of Europe

Alexandre Custaud  
*Consultant*  
IB Consultancy

Perrine Daniel  
*Coordination Manager EU & NATO*  
Thales

Atu Darko  
*Public Affairs Officer*  
NATO



Robin Davies  
*Head of EU Cultural Relations Team*  
British Council

Marta De la Certa  
*Coordinator*  
European Network of NGOs in Afghanistan (ENNA)

Yvan De Mesmaeker  
*Secretary General*  
European Corporate Security Association (ECSA)

Pauline Delleur  
*Public Affairs Officer, Office of the Chairman*  
NATO - Military Committee

Guido Delvoy  
*Global Account Manager NATO*  
Cisco Systems Belgium

Eleni Dima  
*Project Assistant*  
Security & Defence Agenda (SDA)

Jonathan Dowdall  
*Policy Analyst & Market Development*  
Security Europe

Paul Flaherty  
*Deputy Permanent Representative*  
Joint Delegation of the United Kingdom to NATO

Christian Forstner  
*Director*  
Hanns-Seidel-Stiftung

Piers Fotiadis  
*EU Policy Analyst*  
DeHavilland Europe

Jean Fournet  
*Former Assistant Secretary General, NATO*

Anna-Karin Friis  
*Freelance Journalist*

Octávia Frota  
*Senior Advisor*  
Conrad International

Karolina Gasinska  
*Student*  
University of Uppsala

Andrea Ghianda  
*Project Manager*  
Security & Defence Agenda (SDA)

Zoltan Gidaly  
*Seconded National Expert*  
Council of the European Union

Daniel Giorev  
*Member of Cabinet*  
European Commission  
Cabinet of EU Commissioner for International Co-  
operation & Humanitarian Aid Kristalina Georgieva

Laurent Giquello  
*French National Expert*  
NATO - Air Command and Control System  
Management Agency (NACMA)

Henning Häder  
*Project Assistant*  
Security & Defence Agenda (SDA)

Lt.Col. Guy Hanouille  
Emerging Security Challenges Division  
NATO

Laura Harbidge  
*Telecoms Attaché*  
Permanent Representation of the United Kingdom  
to the EU

Michael Hartinger  
*Project Officer, capability development planning*  
European Defence Agency (EDA)

Beatrice Hasani  
*Project Assistant, SDA*

Dan Hass  
*Associate General Counsel*  
United States Air Force, Office of General Counsel

Tal Hasson  
*EU Business Development Manager*  
PwC

Filip Haugland  
*Founder*  
FH Risk Foresight

Cristina Havris  
*Second Secretary*  
Permanent Representation of Romania to the EU

Capt. Denis Heimferte  
*Department Deputy Head, Strategic Analysis*  
NATO

Christopher Helbig  
*Assistant to the Deputy Secretary General*  
European People's Party (EPP)

Ernest J. Herold  
*Account Manager, NATO*  
IBM Belgium

Balazs Honti  
*Analyst*  
IB Consultancy

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

Andrea Walter Isoldo  
*Business Development - EU and NATO*  
Elsag Datamat

David Itier  
*Public Affairs*  
Commissariat à l'Energie Atomique (CEA)

Joanna Jaskowiak  
*Administrator, Civil Protection*  
Council of the European Union  
DG for Justice & Home Affairs

Tonje Johansen  
*Consultant*  
Innovation Circle

Karli Johnston  
*Strategic Intelligence Analyst,*  
*Intelligence Unit of the Office of Security*  
NATO

Tim Kaiser  
*Account Manager NATO*  
Hewlett Packard Belgium

Gustav Kalbe  
*Deputy Head of Unit for Trust and Security*  
European Commission  
DG for Information Society & Media

Ashish Katkar  
*Diplomat (on sabbatical)*  
United States Department of State (DOS)

Janos Kendernay  
*Expert*  
European External Action Service (EEAS)  
Directorate Conflict Prevention and Security Policy

Megan Kenna  
*Programme Assistant*  
European Policy Centre (EPC)

Albert W. Klein Jr.  
*Attorney Advisor*  
United States Mission to NATO

Bogumiła Krakowska  
*Diplomat*  
Permanent Representation of Poland to the EU

Jean Labrique  
*Secretary General*  
Western Defense Studies Institute

Jean-Marie Lhuissier  
*Marketing & Sales Director for EU-NATO,  
Naval Business*  
Thales

Pawel Lisiak  
*Financial Officer*  
European Commission  
DG for Agriculture and Rural Development

Dora Loydl  
*Policy Officer*  
European Commission  
DG for Energy

Ioana Lung  
*Project Officer*  
Centre for European Studies (CES)

Isabelle Maelcamp d'Opstaele  
*Commercial Specialist*  
Mission of the United States of America to the EU

Mauro Marchisotti  
*Institutional Relations Director*  
Iveco Special Vehicles

Pauline Massart  
*Senior Manager*  
Security & Defence Agenda (SDA)

Zurab Matcharadze  
*European Correspondent*  
Resonance Daily Newspaper

Giles Merritt  
*Director*  
Security & Defence Agenda (SDA)

Christine Michelier  
*Manager*  
KfW Group Liaison Office to the EU

H.E. Dr. Branislav Milinkovic  
*Ambassador*  
Mission of Serbia to NATO

Stanislava Mladenova  
*Business Analyst, Executive Management Division*  
NATO

Gabriel Moldoveanu  
*Counsellor*  
Delegation of Romania to NATO

Annalisa Monaco  
*Director EU and NATO Relations*  
The Boeing Company

Valérie Moutal  
*TEN-T Project Manager*  
European Commission  
Trans-European Transport Network Executive  
Agency (TEN-T EA)

Jens Naujeck  
*Coordinator, Brussels Office*  
International Criminal Police Organization  
(INTERPOL)

Kasper Borg Nielsen  
*Counsellor*  
Permanent Representation of Denmark to the EU

Martin Nitsche  
*Global Business Development Executive*  
IBM Deutschland GmbH

Elisa Oezbek  
*Consultant, ESC-Counterterrorism Section*  
NATO

Harriet P. Pearson  
*VP Security Counsel & Chief Privacy Officer*  
IBM Corporation

Antonio Palu  
*Junior Assistant*  
Finmeccanica S.p.A.

Dragos Peica  
*Head of Section Methodology, Quality Assurance & Risk Management*  
European Commission  
DG for Research and Innovation

Raluca Peica  
*Project Manager*  
NATO

Vivien Pertusot  
*Research Fellow*  
Carnegie Europe

Frans Picavet  
*Global NCO Ambassador*  
IBM Belgium

Aneta Podsiadla  
*EU Security and Privacy Policy Manager*  
TechAmerica Europe

Ekaterina Poletaeva  
*Attaché to the Cultural Department*  
Embassy of Russia to Belgium

Zoltan Precsenyi  
*Government Relations Manager*  
Symantec Corporation

Andrew Proudlove  
*Senior consultant*  
IB Consultancy

Neil Robinson  
*Senior Analyst*  
Rand Europe - Brussels

Rear Adm. Jacques Rosiers  
*President*  
Euro-Atlantic Association of Belgium

Lt. Col. Fernand Rouvroi  
*R&T Domain Manager*  
Royal Higher Institute for Defence, Belgium

Diego Ruiz Palmer  
*Head of the Strategic Analysis Capability*  
Emerging Security Challenges Division  
NATO

Michel Savary  
*Police Expert*  
Crisis Management and Planning Directorate  
European External Action Service (EEAS)

Donatella Scatamacchia  
*Journalist*  
Greennews

Kai Schaefer  
*Programme Manager*  
European Commission  
DG for Development and Cooperation  
EuropeAid (DEVCO)

Col. (res) Thomas H. A. Schneider  
*Head of International Affairs*  
European Association for Coal and Lignite  
(EURACOAL)

Vincent Schryvers  
*Corporate QHSE Manager*  
Tractebel Engineering International

Corinna Schulze  
*Governmental Programs Executive*  
IBM Belgium

Svetlana Sergeeva  
*Assistant*  
Human Rights Without Frontiers

Emanuele Sgherri  
*Former European Commission official*  
DG Budget and Financial Affairs

Jamie Shea  
*Deputy Assistant Secretary General*  
Emerging Security Challenges Division  
NATO



Mircea Simion  
*Diplomatic Counsellor*  
Embassy of Romania to Belgium

Aldo Siragusa  
*Honorary Head of Division*  
Council of the European Union

René J. Steiner  
*Administrator*  
European Commission  
DG Human Resources and Security

Andreas Strauss  
*Counsellor, Military Affairs*  
Mission of Austria to NATO

Paul Sturm  
*Programme Officer*  
International Security Information Service Europe  
(ISIS Europe)

Cecilia Szenes  
*Second Secretary*  
Delegation of Hungary to NATO

Nagayo Taniguchi  
*Journalist*  
Sentaku/SEKAI

György Tatar  
*Head of Unit for support of Foreign Affairs Council*  
Council of the European Union

Bryony Taylor  
*Action Officer*  
NATO

Tunc Tekoglu  
*Freelance Journalist*  
DeHavilland Europe

Brooks Tigner  
*Chief Policy Analyst & Head of Technical Studies*  
Security Europe

Gert Timmerman  
*Defence Analyst*  
Ministry of Defence, The Netherlands

Manuela Tudosia  
*Advisor*  
Polit Bureau International

Mustafa Ulusoy  
*President, EU Affairs Consultant*  
EuroAcademic

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

Yves Van Seters  
*Media Relations Manager*  
IBM Belgium

Ivo Veenkamp  
*Director for Policy and Strategy*  
National Coordinator for Counterterrorism,  
The Netherlands (NCTB)

Vyta Vinciene  
*CEO*  
E-Projects Centre (EPC) for Security and Defence

Jelena Von Helldorff  
*Vice-President*  
Institute for International Assistance and Solidarity

Alexander von Lingen  
*Chair*  
EquipEuropa

Kostyantyn Voytovsky  
*Counsellor*  
Mission of Ukraine to NATO

Peiran Wang  
*Visiting Scholar*  
Brussels Institute of Contemporary China Studies

Richard Wright  
*Director Conflict Prevention and Security Policy*  
European External Action Service (EEAS)  
Directorate Conflict Prevention and Security Policy

# The SDA is proud to present its recently extended advisory board

Our advisory board represents a diversified group of high level decision makers, combining top level expertise and experience in the security and defence domain.



Gen. Stéphane Abrial,  
Supreme Allied Commander Transformation  
NATO



Pascale Andréani,  
Ambassador, French Delegation to NATO



Claude-France Arnould  
Chief Executive, European Defence Agency  
(EDA)



Patrick Auroy  
Assistant Secretary General for Defence Investment, North Atlantic Treaty Organisation  
(NATO)



Alyson Bailes  
Visiting Professor, University of Iceland and  
Former Political Director,  
Western European Union (WEU)



Jean-François Bureau  
Contrôle Général des Armées,  
Ministry of Defence, France



Rik Coolsaet  
Head of the Department of Political Science,  
Ghent University



Robert Cooper  
Counsellor, European External Action Service  
(EEAS)



Gilles de Kerchove  
EU Counter-Terrorism Coordinator  
Council of the European Union



Admiral Gianpaolo Di Paola  
Chairman of the Military Committee  
NATO



Ambassador Hüseyin Diriöz  
Assistant Secretary General for Defence Policy and Planning  
NATO



Dumitru Sorin Ducaru  
Ambassador, Delegation of Romania to NATO



Christian Ehler  
Member of the Committee on Foreign Affairs  
European Parliament



Cristina Gallach  
Head of Unit Communications in the Directorate General for  
Press, Communication and Transparency,  
Council of the European Union



Bates Gill  
Director, Stockholm International Peace Research Institute  
(SIPRI)



Ana Maria Gomes  
Member of the Subcommittee on Security and Defence,  
European Parliament



Edward Hanlon  
President, Raytheon International Europe



Scott A. Harris  
President, Continental, Lockheed Martin Global, Inc.



Karel Kovanda  
Governor and EU Representative,  
Asia-Europe Foundation



Ģirts Kristovskis  
Minister of Foreign Affairs, Latvia



Lt. Gen. David Leakey  
Former Director General of the European Union  
Military Staff



Janusz Onyszkiewicz  
President of the Council of the Euro-Atlantic Asso-  
ciation, Poland



Stephen Phipson  
President, Smiths Detection International



William P. Pope  
Senior Advisor for Europe,  
Permanent Mission of the United States to the  
United Nations in New York



Jamie Shea  
Deputy Assistant Secretary General for Emerging  
Secretary Challenges  
NATO



Gen. Sir Rupert Smith  
Former Deputy Supreme Commander Allied  
Powers Europe



Walter Stevens  
Permanent Representative of the Kingdom of  
Belgium to the Political and Security Committee  
of the EU and to the Western European Union



Leendert van Bochoven  
NATO Account Executive and Defence Leader for  
Global Business Services, IBM Nederland B.V.



Geoffrey Van Orden  
Member of the Subcommittee on Security and  
Defence, European Parliament



Lt. Gen. Ton van Osch  
Director General of the European Union Military Staff



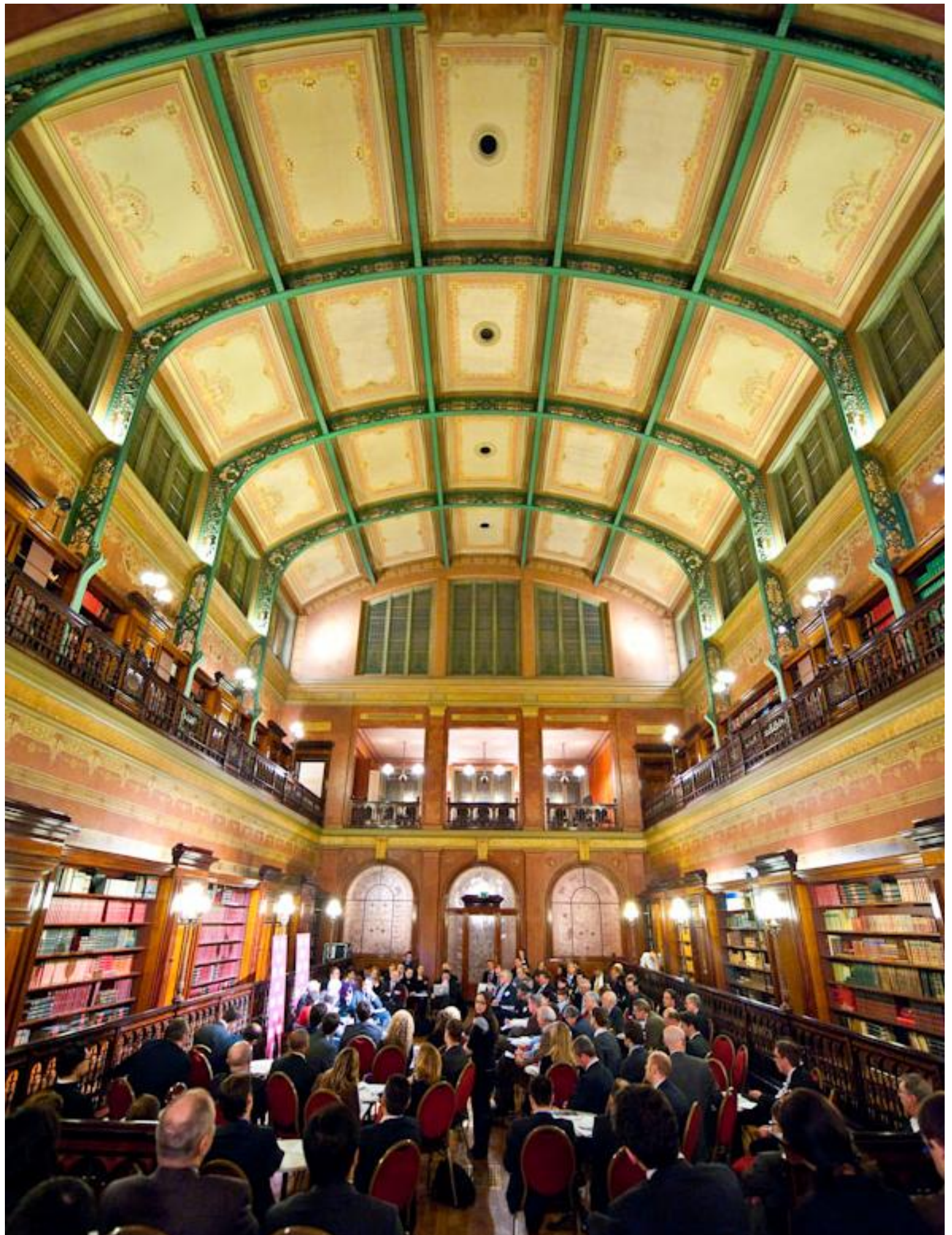
Veronika Wand-Danielsson  
Ambassador, Mission of Sweden to NATO



Nick Witney  
Senior Policy Fellow  
European Council on Foreign Relations (ECFR)











IBM and the IBM logo are registered trademarks of International Business Machines Corporation in the United States and/or other countries. Other company, product and service names may be trademarks or service marks of others. ©2006 IBM Corporation. All rights reserved.

The background of the advertisement features a black and white photograph of two soldiers in silhouette. They are wearing helmets and carrying equipment, with one soldier in the foreground holding a rifle. The scene is set against a bright, hazy sky, creating a stark contrast.

# YOU CAN RESPOND TO YOUR ORGANIZATION'S HIGH EXPECTATIONS

European defense ministries and NATO face difficult challenges at every level. Decentralized organizational and operational structures. Need for improved productivity and performance. Escalating operational costs and budget shortfalls. Security issues. How do you respond? How do you transform?

Enter IBM. With deep experience in helping military forces all around the world, IBM offers a unique combination of innovative industry insights and proven end-to-end technology solutions to help you be a more responsive and flexible organization. Integrating processes, information and technology across departments and agencies. Transforming the way you work, collaborate and deliver services. All in a cost effective and secure manner. For more information visit [ibm.com/government](http://ibm.com/government)

The Security & Defence Agenda is Brussels' only specialist defence and security think-tank. It brings together top-level representatives from NATO, the European institutions, national governments and parliaments, NGOs, industry, academia and the media in debates, conferences and discussion papers.

**SDA Co-Presidents**



**Jaap de Hoop Scheffer**  
former Secretary General  
of NATO

**Javier Solana**  
former EU High High  
Representative for Common  
Foreign and Security Policy



# SAFEGUARDING EUROPE



**THE SDA ATTRACTS TOP INTERNATIONAL SECURITY EXPERTS**

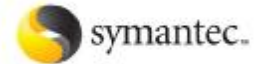
Last year the SDA held 16 events, debates and meetings, at which over 280 senior defence and security leaders took the floor. A ground-breaking innovation was the SDA's Security Jam, which gathered 4,000 security & defence specialists from 124 countries for a five-day online discussion. In 2011 the SDA will cover topics ranging from the reform of NATO and relations with Russia to cybersecurity and energy security—speakers this spring will include General Abrial, NATO Supreme Allied Commander Transformation, Ivan Bizjak, EU Council Director-General for Justice and Home Affairs, Peter Zangl, European Commission Director General for Humanitarian Aid & Civil Protection, Gabor Iklody, NATO Assistant Secretary General for Emergent Threats, and Craig Mundie, CTO of Microsoft.

For more information on SDA programmes and membership, visit  
[www.securitydefenceagenda.org](http://www.securitydefenceagenda.org)





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



For further information on SDA membership, contact us at:  
Tel: +32 (0)2 739 1582 | E-mail: [info@securitydefenceagenda.org](mailto:info@securitydefenceagenda.org)

The SDA gratefully acknowledges the generous support of the following governments:  
Belgium | Czech Republic | Finland | France | Italy | Netherlands  
Qatar | Romania | Russia | Sweden | Turkey | United States | United Kingdom

## 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](mailto:info@securitydefenceagenda.org)  
[www.securitydefenceagenda.org](http://www.securitydefenceagenda.org)  
Twitter: <http://twitter.com/secdefagenda>