



European Commission  
DG Information Society and Media

## SDA Report

Evening debate—27 April, 2011  
Bibliothèque Solvay, Brussels

# Controlling the Internet: Balancing limits with guarantees of citizens' freedoms



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.

**A *Security & Defence Agenda* Report**

**Rapporteur: Jonathan Dowdall**

**Photos: Philippe Molitor**

**Date of publication: May 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>

## Controlling the internet: Balancing limits with guarantees of citizens' freedoms

### Table of contents

Speakers and moderator	p.3
Introduction	p.4
The nature of the challenge	p.4
Europe's role in forming an international code of conduct	p.6
Accessibility and the question of the "kill-switch"	p.7
Security vs. freedom - the fundamental balancing act	p.8
Conclusion	p.9
List of participants	p.11



## Controlling the internet: Balancing limits with guarantees of citizens' freedoms

### Evening debate

Wednesday 27 April 2011  
Bibliothèque Solvay, Brussels

The so-called 'Twitter' or 'Web 2.0' revolutions in the Arab world have sparked fierce debate on the right of governments to shut down the internet. This has been paralleled by criticism of Iran and China for their use of social media to track political protesters and for propaganda. The storage of data on these platforms greatly increases public and private vulnerabilities to attack. Does switching off the internet constitute a breach of freedom of speech, and if so, should the EU develop capabilities to prevent this? Does NATO's cybersecurity policy include this issue and what kind of actions or sanctions might be considered? Could an EU platform for cooperation between public and private actors contribute to regulating cyberspace, and could such a platform enable governments to stay up to speed with technological developments?

#### Speakers



**Suleyman Anil**  
*Head, Cyber Defence Section, Emerging Security Challenges Division (ESCD)*  
North Atlantic Treaty Organisation (NATO)



**Joe McNamee**  
*Advocacy Coordinator*  
European Digital Rights (EDRI)



**Robert Madelin**  
*Director-General for Information Society and Media*  
European Commission

#### Moderator



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



**Erika Mann**  
*Executive Vice President*  
Computer & Communications Industry Association  
*Member of the Board of Directors*  
Internet Corporation for Assigned Names and Numbers (ICANN)

## Controlling the internet: Balancing limits with guarantees of citizens' freedoms



### Introduction

In the wake of the “Arab Spring” uprisings, authoritarian regimes across the Middle East have demonstrated a willingness to use internet shut-downs and restrictions to quell unrest. Noting that “this is by far the most innovative debate we have held on cyber issues”, SDA Director **Giles Merritt** nonetheless asserted that the increased “nature and scope of developments” related to the manipulation of the internet by governments deserves concerted attention.

Spurred by pressing questions about internet resilience and fundamental human rights raised by events in the Arab world, participants from across the EU institutions, NATO, NGOs and industry gathered to discuss Europe’s role in balancing security and freedom in cyber-space. During a vigorous and often heated debate, participants engaged with how to develop principles and codes of conduct for managing the internet; the necessity of government’s maintaining an internet “kill-switch” and the potential risks involved in prioritizing security over freedom in this vital domain.

### The nature of the challenge

The panellists began by outlining their vision of the issues at play when Europe approaches

internet security and freedoms. **Robert Madelin**, Director General for DG Information Society and Media of the European Commission, saw a fundamental need to spread European values for managing the internet. He asserted that it was important to “nurture our view of the internet and its freedoms around the world” in the face of internet repression abroad. In Madelin’s view, foreign actors will only come to accept a European ethos of internet openness “if the EU can keep a strong stance on internet freedom” here at home.

*“It is important to nurture our views of the internet and its freedoms around the world.”*

However, he continued, the real challenge was deciding how broadly should the issue be scoped asking “Should we discuss only about catastrophic threats or also surveillance or censorship practises?” and how the EU should achieve this objective. “Should we as a European Union be proactive, or simply say we will react appropriately when we see a problem emerge?” Madelin queried. Perhaps equally as importantly, he asked participants to consider “what tools do we have, and what are the rules for their use” in the internet domain.



## Controlling the internet: Balancing limits with guarantees of citizens' freedoms



Focusing on the national security implications of these questions, **Suleyman Anil**, Head of the Cyber Defence Section in NATO's Emerging Security Challenges Division, agreed that the question of tools was an important one. "The internet is inherently vulnerable" to attack, Anil explained, due to its systemic openness and the rapid advance of technology. It could thus "endanger our critical national infrastructures and services", a threat which behoves Europe to "improve present resilience, as well as our potential responses to internet traffic that is disruptive to wider access". Taking steps to ensure resilience to disruption should thus be Europe's priority, because "the internet has become a national asset where our national interest lies", Anil concluded.

*"our security as a fundamental human right is put at risk when our access to the internet is defined by the whims of commercial actors."*

However, this national security approach ran contrary to the views of **Erika Mann**, Executive Vice President of the Computer & Communications Industry Association and a Member of the Board of Directors for ICANN. In Mann's opinion, the internet's role as a "democratic instrument" is currently guaranteed by the ingenuity and innovation of the ICT industry. Introducing excessive European

legislation thus risks over-playing the security threat, and strangling innovation. The internet is "a stimulating and fascinating instrument - we need to look at this in these terms", Mann cautioned. "If you come in with a heavy hand because of threats, you are misjudging the security environment". She summarised that "we need to build our European internet on a system of openness, not restriction".

*"We need to build our European internet on a system of openness, not restriction."*

**Joe McNamee**, Advocacy Coordinator for European Digital Rights, added that "if we don't establish principles and stick rigorously to them" when it comes to freedom of internet access, "we'll never provide the thought leadership needed to guide international actors on this issue". McNamee also cautioned that Europe is drifting into dangerously restrictive tendencies. Expressing concern at the faith placed in industry actors to secure the internet by the other panellists, McNamee warned that "our security as a fundamental human right is put at risk when our access to the internet is defined by the whims of commercial actors". "Bad regulation", he added, "is oxygen for criminals and poison for our fundamental rights". Europe will thus need to consider extremely carefully which

## Controlling the internet: Balancing limits with guarantees of citizens' freedoms



safeguards, tools and legal instruments it feels are appropriate to guarantee the security of the internet without falling into this trap.

### Europe's role in forming an international code of conduct

These diverse views drew a range of comments from the floor about the potential role of Europe in this global process. **Martin Schmidt**, Counsellor at the Delegation of Germany to NATO, asked what the implications of Europe being a "global norm maker" were in relation to the policies of India, China, and other large states outside of the traditional Western security loop. **Richard Allan**, Director of Policy for Europe at Facebook, added that "many principles and standards that balance access and freedom already exist", for instance, in the EU Charter of fundamental rights, and in national legal systems as practiced by some member states. Could these models form the basis of an international agreement on internet conduct?

Madelin agreed that international partners will form an important part of any future code of conduct related to internet freedoms. "Europe can't fix these things on its own", he observed, and "you can't argue with the global nature of the internet". In this context, Europe's role will be to develop global norms negotiated on a global scale, not via strict

European trend setting. This process may not be easy, or fast, but "I don't think we can do better than the 'Bretton Woods' style cooperative rule-making we have today", Madelin concluded. Currently, the EU is also exploring in which circumstances it could intervene to make sure that the freedoms, rights and possibilities allowed by a unhindered access to the internet are preserved.

*"Europe can't fix these things on its own... you can't argue with the global nature of the internet."*

McNamee, whilst agreeing that "we have the biggest, strongest, most credible voice for norm-setting in the world", strongly disputed this opinion. The naturally slow and incremental nature of international treaty-making is, in McNamee's view, being used as an excuse for introducing "interim permanent solutions" that contravene human rights. For instance, McNamee elaborated, how can Europe maintain that its long-term goal is a global standard based on freedom, when it "enters into trade deals with third party nations that will allow people to be cut off from the internet in an extrajudicial way"? This hypocrisy renders Europe's efforts hollow, and requires rapid rectification, he concluded.

Countering this argument, Madelin main-

## Controlling the internet: Balancing limits with guarantees of citizens' freedoms



tained that in order to “avoid irrelevance at this crucial moment” in the development of the internet, Europe would need “to learn to live with inconsistencies” on the long road to a global set of standards. In the face of online criminality such as child pornography and fraud, Europe does indeed use tools that sometimes breach strongly held values, Madelin agreed. However, European citizens will simply not tolerate a “laxist and laissez-faire attitude” towards such crimes. He also warned that ‘freedom’ is “an absolute, and you can’t deliver that through a policy”. So, a better approach would be to place values such as openness and accessibility at the centre of a long-term vision of where Europe is going regarding the internet, regardless of short-term inconsistencies.

### Accessibility and the question of the “kill-switch”

**Frank Asbeck**, Principal Counsellor for Security and Space Policy at the European External Action Service, asked whether the “high probability of not being caught following a cyber attack” challenged the European emphasis on accessibility. If tracing internet users is considered against European standards, “how do you improve cyber security without employing systems where you are obliged to be verified or registered?”, the EU official queried.

Responding to this question, Mann reminded participants that there was a need for proportionality in Europe’s response to internet disruptions. “We need to understand current security levels” which consists of “daily attacks of varying levels of severity”, she expounded. Tracking all users would be an exaggerated response to this threat level. McNamee also agreed that Europe should not consider restrictive online monitoring in the name of security. “Would we want Iran or China to introduce mandatory online attribution? If not, we should not give them an example”, he warned.

*“Would we want Iran or China to introduce mandatory online attribution? If not, we should not give them an example.”*

What is more, restricting accessibility in the name of security is in fact counter-productive, explained Mann. In order to handle potential disruption, information must flow freely. “Awareness is only guaranteed with information”, she claimed. “Security depends on freedom of access [to information] - you do not get high security without such freedom”.

Anil also agreed with Mann that access to information was a more effective way of trac-



## Controlling the internet: Balancing limits with guarantees of citizens' freedoms



ing disruptions than heavy-handed monitoring. “The main reason we do not have exact pinpointing of the traffic [from attacks] is because we did not have international cooperation” for information handling. Contrary to people’s fears, Anil explained, “there is no problem of attribution” within friendly nations, but only when network data crosses behind the borders of uncooperative third party nations. Building global partnerships for information-sharing is thus a stronger method of tracking attacks than the forced registration of users, the NATO official concluded.

*The “internet has to be open, yes, but we need to be prepared to deny the opportunities of the internet to actors who wish us harm”*

However, the panellists were more divided over another potential tool for handling disruptive internet attacks: the ability for governments to shut-down the internet within their borders, or a “kill-switch”. This method has particular significance in relation to the Arab Spring, after the Egyptian Government used its kill-switch to silence dissent, at the height of political unrest in the country.

Mann believed there are no security threats that require such an extreme reaction, calling

its use “stupid”, and against European values. Giles Merritt also asked participants if shutting down such a vital economic and social lifeline was not the same as “committing suicide to avoid being murdered?”

Anil strongly disagreed, however claiming “we cannot ignore that we need switches in place”. His argument was built on the 2007 distributed denial of service (DDoS) attack unleashed on Estonia, which rendered the country’s administrative and telecommunications systems un-useable. The Estonian selective switch-off of international internet connections granted them a vital respite. The “internet has to be open, yes, but we need to be prepared to deny the opportunities of the internet to actors who wish us harm”, Anil argued. Indeed, in the NATO official’s opinion, “quite a few nations could not survive 1/10<sup>th</sup> of what attacked Estonia”. Without extreme measures such as kill-switches, Europe could be very vulnerable to DDoS disruptions, and he asked participants to bear this in mind.

### **Security vs. freedom - the fundamental balancing act**

These sharp divergences of opinion highlighted the inherent balancing act between security and freedom in the cyber-domain. In order to gauge perspectives on this balance, the chairman asked the assembled partici-

## Controlling the internet: Balancing limits with guarantees of citizens' freedoms



participants to give a show of hands casting their votes either in favour of the priority of security, or freedom. The vote demonstrated an overwhelming focus on freedom amongst

*“You only swat a fly with a sledgehammer when you have to, but later you look for a flyswatter.”*

those present, but it was also agreed this two-way vote did not capture the depth of the issue.

Invited to explain his position, **Zoltan**



**Precsenyi**, Government Relations Manager for Symantec Corporation, explained he had voted “on the assumption that one of my fundamental freedoms is security”, under the EU Charter of fundamental rights. **Branislav Milinkovic**, Serbian ambassador to NATO, agreed that “all mediums” are protected as vehicles of free speech by the Charter. This means that there is no need to choose between security or freedom; EU law demands that member states assure both, no matter how difficult this may be.

### Conclusion

Given this, and the clashes of opinion noted during the debate, it became clear Europe has a long way to go before it can satisfactorily prove it is balancing security limitations and guarantees of citizens freedoms. EU members may not resort to authoritarian censorship online as in so many countries worldwide, but there are nonetheless some challenging ambiguities in current policy and practice.

However, participants and panellists did end on a note of optimism. **Ernest Herold**, NATO Account Manager for IBM Belgium, noted that the current inconsistencies between internet policing tools and values will eventually be rectified by new technology. “The challenges that industry can solve on this policy debate have been overlooked”, he sug-

## Controlling the internet: Balancing limits with guarantees of citizens' freedoms



gested. “You only swat a fly with a sledgehammer when you have to, but later you look for a flyswatter”. It was thus suggested that the fears of freedom will naturally be assuaged as more sophisticated and targeted online tools became available.

Indeed, all of the panellists agreed that with the challenges of balancing freedom and security came the opportunity to build a better online world. “The internet is a blank page, for Europe to reinvent itself on”, Madelin reminded participants. Mann added that “the internet teaches us that there is an incredible amount of intelligence available - sometimes with a bad face, but often good”. In her opinion, the progression of internet freedoms would be best assured by emphasising the use of this “good” intelligence. Despite the security dangers, it is important to bear in mind the internet’s benevolent role in spreading democracy and highlighting injustice in the Arab world and world-wide. As McNamee concluded, “we can’t destroy what makes the internet good because of what makes it bad”.

## Controlling the internet: Balancing limits with guarantees of citizens' freedoms

### List of participants

**Enver Akhmedov**

*Senior Counsellor*

Permanent Mission of the Russian Federation to NATO

**Selen Akses**

*Junior Researcher*

Economic Development Foundation (IKV)

**Richard Allan**

*Director of Policy for Europe*

Facebook

**Suleyman Anil**

*Head of Office, Computer Incident Response Capability Coordination Centre*

North Atlantic Treaty Organisation (NATO)

**Frank Asbeck**

*Principle Counsellor for Security and Space Policy*

European External Action Service (EEAS)

**Mohamed-Raja'l Barakat**

*Expert*

**Giuseppe Belardetti**

*Programme Director*

Atlantic Treaty Association (ATA)

**Andreas Belschner**

*Account Director Government, EU and NATO*

Orange Business Services

**Juliette Bird**

*First Secretary Security and Terrorism*

Permanent Representation of the United Kingdom to the EU

**Jakub Boratynski**

*Head of Unit, Fight against organised crime*

European Commission

DG Home Affairs

**Adam Bowering**

*Assistant*

Political Intelligence

**Alejandro Cainzos**

*Policy Officer, US and Canada Division*

European External Action Service (EEAS)

**Geert Cami**

*Co-Founder & Director*

Security & Defence Agenda (SDA)

**Giovanni Colombo**

*Consultant*

Hill & Knowlton International Belgium

**Amelie Coulet**

*Associate*

APCO Worldwide Brussels Office

**Anna Dahlman**

*Project Assistant*

Unrepresented Nations and Peoples Organisation (UNPO)

**Claire Davenport**

*Journalist on Financial Services*

EurActiv.com

**Charles de Marcilly**

*Director of the Brussels Office*

Fondation Robert Schuman

**Rebeca De Sancho Mayoral**  
*Communication Financial Officer*  
European Commission  
DG Enlargement

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

**Irini Dimitriou**  
*Assistant*  
Mission of Austria to NATO

**Daniel Dimov**  
*Assistant*  
European Digital Rights (EDRI)

**Andrea D'Incecco**  
*Head of Policy*  
European Internet Service Providers Association  
(EUROISPA)

**Hervé Dupuy**  
*Member of Cabinet, Justice, Fundamental Rights  
and Citizenship*  
European Commission  
Cabinet of Commissioner Neelie Kroes

**Philip Eder-Levacher**  
*Senior Account Executive*  
Fleishman-Hillard

**Chris Ehrman**  
*Assistant*  
North Atlantic Treaty Organisation (NATO)

**Alessandra Falcinelli**  
*Policy Officer*  
European Commission  
DG Information Society & Media

**Giuseppe Fiore**  
*Assistant*  
Permanent Representation of Italy to the EU

**Magnus Franklin**  
*Journalist*  
MLex Market Intelligence

**Oliver Fueg**  
*Policy Officer*  
European Commission  
DG Information Society & Media

**Karolina Gasinska**  
*Analyst*  
IB Consultancy

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

**Andrea Glorioso**  
*Policy Officer*  
European Commission  
DG Information Society & Media

**Sarah Grauls**  
*Executive*  
Brunswick Group

**Peter Grunditz**  
*Brigadier (retired), Swedish Armed Forces*

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

**Juliane Heil**  
*Desk Officer, Justice*  
Representation of Brandenburg to the EU



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

**Julia Kulakovska**  
*Second Secretary*  
Mission of Ukraine to NATO

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

**Jean Labrique**  
*Secretary General*  
Western Defense Studies Institute

**Tuija Hirvonen**  
*Consultant*  
Cognizant

**Tina Liebherr**  
*Assistant*  
Information Office Mecklenburg-Vorpommern

**Glen Hodgson**  
*Director, Energy, ICT, Transport and Environment*  
Hill & Knowlton International Belgium

**Joe Litobarski**  
*Project Manager, Debating Europe*  
Europe's World

**Tim Kaiser**  
*Account Manager NATO*  
Hewlett Packard Belgium

**Diane Luquiser**  
*General Manager*  
Top Strategies

**Niels Karssen**  
*Consultant*  
Avisa Partners

**Ms. Siobhan MacDermott**  
*Chief Policy and Investor Relations Officer*  
AVG Technologies

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

**Robert Madelin**  
*Director General*  
European Commission  
DG Information Society & Media

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

**Erika Mann**  
*Vice-President*  
Computer & Communications Industry  
Association (CCIA)

**Slaven Klobucar**  
*Secretary General*  
European Liberal Youth (LYMEC)

**Lorenzo Marchese**  
*Assistant to the Secretary General*  
European Liberal Youth (LYMEC)

**Agnieszka Konkol**  
*Minister Counsellor*  
Polish Ministry of the Interior and Administration

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

**Chiara Mazzone***Policy Officer*

Représentation de la Région  
Provence-Alpes-Côte d'Azur à Bruxelles

**Eva McKeown***Assistant*

European Internet Services Providers Association  
(EuroISPA)

**Joe McNamee***Advocacy Coordinator*

European Digital Rights (EDRI)

**Natalia Melnyk***Second Secretary*

Mission of Ukraine to NATO

**Giles Merritt***Director*

Security & Defence Agenda (SDA)

**Marta Mikłaszewicz***Assistant*

North Atlantic Treaty Organisation (NATO)

**H.E. Dr. Branislav Milinkovic***Ambassador*

Mission of Serbia to NATO

**Maia Milusheva***Assistant, ICTM-EM*

North Atlantic Treaty Organisation (NATO)

**Matteo Minchio***Correspondent*

Lo Spazio della Politica

**Gabriel Moldoveanu***Counsellor*

Delegation of Romania to NATO

**Valérie Moutal***TEN-T Project Manager*

European Commission  
Trans-European Transport Network Executive  
Agency (TEN-TEA)

**Yukio Nakajima***First Secretary*

Mission of Japan to the EU

**Jens Naujeck***Coordinator*

International Criminal Police Organization  
(INTERPOL)

**Martin Nitsche***Global Business Development Executive*

IBM Deutschland GmbH

**Elis Nuh***Assistant*

Turkish Industry and Business Association  
(TÜSIAD)

**Ozge Ogutcu***Assistant, Public Diplomacy Division*

North Atlantic Treaty Organisation (NATO)

**Maria Okkonen***Journalist*

Science & Technology Review

**Valery Oknyanskiy***Counsellor*

Permanent Mission of the Russian Federation to  
NATO

**Giuseppe Paladino***Sales Manager*

Engineering Ingegneria Informatica S.p.A.

**Cesare Marco Pancini**  
*Senior Policy Counsel*  
Google

**Kirsten Pasedag**  
*Policy Officer, Interior*  
Representation of Brandenburg to the EU

**Raluca Peica**  
*Project Manager, Executive Management Division*  
North Atlantic Treaty Organisation (NATO)

**Antti Peltomäki**  
*Deputy Director General*  
European Commission  
DG Information Society & Media

**Peter Power**  
*Member of Cabinet, Internal Market (Financial),  
International Cooperation, Humanitarian Aid,  
Transport, Tax & Customs*  
European Commission  
Cabinet of Commissioner Neelie Kroes

**Zoltan Precsenyi**  
*Government Relations Manager*  
Symantec Corporation

**Charles Rault**  
*Director*  
International Security Research and Intelligence  
Agency (ISRIA)

**Jarrett Reckseidler**  
*Political Officer*  
Mission of Canada to the EU

**Timm Rentrop**  
*Legal Officer, EU Labour Law*  
European Commission  
DG Employment, Social Affairs and Inclusion

**Neil Robinson**  
*Senior Analyst*  
Rand Europe - Brussels

**Michael Ruoff**  
*Independent EU Policy Advisor*

**Volkan Sahinkaya**  
*Assistant*  
Turkish Industry and Business Association  
(TÜSIAD)

**Paolo Salieri**  
*Principal Policy Officer*  
European Commission  
DG Enterprise and Industry

**Helen Rebecca Schindler**  
*Senior Analyst*  
Rand Europe - Brussels

**Martin Schmidt**  
*Counsellor*  
Delegation of Germany to NATO

**Moureen Schobert**  
*Project Manager*  
European Organisation for Security (EOS)

**Elsa Schrier**  
*Consultant*  
IB Consultancy

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

**Sandra Silfvast**  
*Research Assistant*  
Mission of Australia to the EU

**Zeka Sizo**

*Administrateur Délégué*  
Les Amis du Monde Entier

**Chelsey Slack**

*Consultant, Emerging Security Challenges Division*  
North Atlantic Treaty Organisation (NATO)

**Col. Wouter Sleurink**

*Staff Officer*  
North Atlantic Treaty Organisation (NATO)

**Tatiana Smirnova**

*Senior Counsellor*  
Mission of the Russian Federation to the EU

**Viorel Stan**

*Attaché, INFOSEC Department*  
Permanent Representation of Romania to the EU

**René J. Steiner**

*Administrator*  
European Commission  
DG Human Resources and Security

**Diliana Stoyanova**

*Assistant*  
European Commission  
DG Information Society & Media

**Andreas Striegnitz**

*Administrator*  
European Parliament

**Katarina Subakova**

*Research Analyst*  
Europe Analytica

**Anna Szatkowska**

*Advisor*  
Permanent Representation of Poland to the EU

**Christof Tatschl**

*Chief of Staff and Military Counselor*  
Mission of Austria to NATO

**Laurent Thomet**

*Defence Correspondent*  
Agence France Presse (AFP)

**Irina Tica-Diaconu**

*Second Secretary*  
Permanent Representation of Romania to the EU

**Ulrich van Essen**

*Head of Unit, Information Assurance*  
Council of the European Union

**Willem van Sluijs**

*Counsellor Home Affairs*  
Permanent Representation of the Netherlands to the EU

**Robby Veders**

*Assistant*  
House of Netherlands Provinces

**Ekaterini Vourka**

*Linguist Administrator*  
Council of the European Union

**Kostyantyn Voytovsky**

*Counsellor*  
Mission of Ukraine to NATO

**Peiran Wang**

*Visiting Scholar*  
Brussels Institute of Contemporary China Studies (BICCS)

**Manharsinh Yadav**

*Second Secretary (Head of Chancellery)*  
Mission of India to the EU

**Lixin Yang**  
*EU Correspondent*  
New Tang Dynasty Television

**Christine Zander**  
*Assistant*  
European Commission  
DG Enterprise and Industry

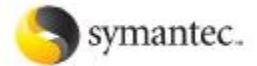
**Marko Ziske**  
*Policy Officer, Justice and Interior*  
Representation of Brandenburg to the EU







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



CENTER FOR STRATEGIC & INTERNATIONAL STUDIES



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

For further information on SDA membership, contact us at:  
Tel: +32 (0)2 739 1582 | E-mail: [info@securitydefenceagenda.org](mailto: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](mailto:info@securitydefenceagenda.org)  
[www.securitydefenceagenda.org](http://www.securitydefenceagenda.org)  
Twitter: <http://twitter.com/secdefagenda>