SDA
SECURITY & DEFENCE AGENDA

Public-private cooperation in cyber-security

Report

Bibliotheque Solvay
30 January 2012

In partnership with:

FINMECCANICA
IBM
McAfee An Intel Company
Microsoft
NATO OTAN
Raytheon
TNO innovation for life
Europe's World THE ONLY EUROPE-WIDE POLICY JOURNAL

A *Security & Defence Agenda* Report
Rapporteur: Jonathan Dowdall
Photos: Philippe Molitor - Gleamlight
Publisher: Geert Cami
Date of publication: February 2012

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

Programme

Policymakers' dinner – 30 January 2012

Bibliothèque Solvay, Brussels, 19:30-21:30

National approaches to cyber-security greatly vary within Europe and around the world. In some countries, legal responsibility to combat piracy rests with internet providers, with technical expertise often greater in the private sector. How much frontline protection should be left to private companies? How good is information-sharing between public institutions and the private sector? Can the creation of new EU-level and international standards improve our cyber-security, and if so what should these entail?

Speakers:

Gábor Iklódy, Assistant Secretary General for Emerging Security Challenges, North Atlantic Treaty Organisation (NATO)
Neelie Kroes, Vice President of the European Commission responsible for the Digital Agenda
Craig Mundie, Chief Research & Strategy Officer, Microsoft
Harry van Dorenmalen, Chairman, IBM Europe

Speakers & moderator

Gábor Iklódy
Assistant Secretary General for Emerging Security Challenges
North Atlantic Treaty Organisation (NATO)

Ambassador Gábor Iklódy is NATO's Assistant Secretary General for Emerging Security Challenges. He is the Secretary General's primary advisor on emerging challenges and their potential implications for the security of the Alliance. The division, which he directs, aims to provide a coordinated approach to the challenges of the 21st century, including terrorism, Weapons of Mass Destruction proliferation, cyber-threats, as well as energy security challenges.

Iklódy joined the Hungarian Foreign Service in 1983. Before taking up his new position at NATO, he worked as Political Director and State Secretary in charge of multilateral issues, a position he was appointed to in 2009, with the main focus on Hungary's 2011 EU Presidency. Between 1999 and 2009, he served as Ambassador in Norway and in Sweden. In between the two (2003-2005), he filled the position of Director General for European Political Cooperation in Budapest.

In 1996, Iklódy headed the Foreign Ministry's Security Policy and Arms Control Department, and from 1997 to 1999 its NATO and WEU Department. From 1990 until 1995, he worked at the Hungarian CSCE/OSCE Mission, from 1992 as deputy head. He was part of the team negotiating and implementing the CFE treaty and was responsible during the 1995 Hungarian OSCE Chairmanship for all activities related to the organization's field missions. In 1989/90, after having returned from his first posting abroad in Romania (between 1986 and 1989), he worked as private secretary to State Secretary Ferenc Somogyi.

Neelie Kroes
Vice President of the European Commission
responsible for the Digital Agenda
European Commission

Neelie Kroes is Vice President of the European Commission responsible for the Digital Agenda for Europe.

Kroes' career started at the Rotterdam Municipal Council, and in 1971 she was elected as a Member of the Dutch Parliament for the liberal VVD party. From 1982 to 1989, she served as Minister for Transport, Public Works and Telecommunication in the Netherlands.

After politics, Kroes was appointed President of Nyenrode University from 1991 to 2000, and served on various company boards, including Lucent Technologies, Volvo, P&O Nedlloyd.

Prior to serving as European Commissioner for Competition from 2004 to 2009, Kroes' charity work included advising the Nelson Mandela Children's Fund and World Cancer Research Fund.

Speakers & moderator

Giles Merritt
Director
Security & Defence Agenda

Giles Merritt is among Brussels' most influential commentators on EU issues. He was a pioneer of the public policy debate on Europe's future, both as a journalist and think-tanker.

Merritt is also the head of the SDA's sister think-tank Friends of Europe, whose debates and reports cover the whole spectrum of non-defence topics of interest to EU-level policymakers, researchers and stakeholders. In addition, he is the editor of the policy journal Europe's World launched in 2005 as an EU-wide platform for debate.

Merritt's work with think-tanks began in the mid-1980s, when he devised and chaired a series of Business Policy Seminars on behalf of the Centre for European Policy Studies (CEPS). He went on to act as Moderator at the French-language debates organised by the Club de Bruxelles, and at many of the conferences held by Aspen Institute Italia. In 1992, he accepted an invitation to be the director of the new Philip Morris Institute for Public Policy Research (PMI), and was responsible for the highly successful series of quarterly Discussion Papers that PMI produced until its closure in 1999.

Craig J. Mundie
Chief Research & Strategy Officer
Microsoft Corporation

Craig Mundie is Chief Research and Strategy Officer of Microsoft Corp. In this role, he oversees one of the world's largest computer-science research organizations, and is responsible for Microsoft's long-term technology strategy. He also directs the company's fast-growing healthcare-solutions business, along with a number of technology incubations. He routinely works with government and business leaders around the world on technology policy, regulation and standards.

Mundie joined Microsoft in 1992. Before his current role, he served as the company's chief technical officer for advanced strategies and policy, working with Chairman Bill Gates to develop the company's global strategies around technical, business and policy issues. Mundie initiated Microsoft's Trustworthy Computing initiative, which has leveraged new software-development practices to improve the security of the company's products. He has also served as Microsoft's principal technology-policy liaison to the US and foreign governments, with an emphasis on China, India and Russia. He serves on the US National Security Telecommunications Advisory Committee and the Task Force on National Security in the Information Age. In April 2009, he was appointed by President Obama to the President's Council of Advisors on Science and Technology.

Mundie started his career in 1970, working on operating-system development for the Data General NOVA at Systems Equipment Corp. (SEC). In 1977, he moved to Data General's advanced development facility, ultimately becoming its director. In 1982, he was one of three co-founders of Alliant Computer Systems Corp., where he held a variety of positions before becoming CEO. He holds a bachelor's degree in electrical engineering and a master's degree in information theory and computer science from Georgia Tech.

Speakers & moderator

Harry van Dorenmalen
Chairman
IBM Europe

Harry van Dorenmalen was appointed chairman of IBM Europe on 1 October 2010. He represents IBM to the EU institutions and other organisations such as NATO and the European Defence Agency on issues of international public policy and business regulation. In this role he also oversees the company's corporate citizenship, environmental affairs, intellectual property, standards development, venture capital and university relations activities across the region. He takes on this responsibility in addition to his role of Country General Manager, IBM Netherlands, a position he has held since 2005.

Van Dorenmalen started his career at IBM in 1982 as a programmer. Since then he has held a series of leadership positions including Vice President of IBM's Industrial Sector business in Europe, Middle East and Africa, responsible for the Automotive and Electronics sector, and Managing Director for IBM's business with Royal Philips Electronics. He has also been Director of IBM's Service Delivery Organisation in Europe and has enjoyed spells in the company's professional services, manufacturing, application development and consulting divisions.

Since December 2010, van Dorenmalen has been Chairman of the Dutch IT industry association, ICT-Office.

Van Dorenmalen holds a degree in Business Administration from the University of Delft.

SDA Director Giles Merritt opened up this high-level policymakers' debate with some tough questions about cyber-security: "What costs are involved, who will bear them? How do we balance between public and private? How do we try and create an international fabric of responsibility?"

Such tough questions defy easy answers, but all of the assembled experts from industry, governments, the EU and NATO agreed on one basic principal. As Vice President of the European Commission responsible for the Digital Agenda Europe Neelie Kroes stated, "we need to exchange good practices, before we run out of time."

Indeed, time is running out, agreed Assistant Secretary General (ASG) for Emerging Security Challenges at NATO, Amb. Gábor Iklódy. He argued that the character of the cyber challenge requires new thinking about defence and security. "We should concentrate a lot more on prevention and resilience, the good old concepts of defence and deterrence do not work," he opined.

"We should concentrate a lot more on prevention and resilience, the good old concepts of defence and deterrence do not work."

Gábor Iklódy

NATO looks at challenges coming from cyberspace from a defence perspective. But it needs to accept that cyber is different from traditional domains, like land, air, sea and space. One key difference stems from the problem of attribution, whereby the perpetrators often remain anonymous. NATO's traditional deterrence power (i.e. deterrence by retaliation) does not really work here. Nonetheless, the problem of attribution is not absolute. In a cooperative international environment, through strong public-private partnership and building on the advances in technology we can cope with the problem.

Cyberspace is a global phenomenon, where there are no boundaries and no distances in time. Cyberspace does not belong to governments, the vast majority of cyber assets are in the hands of private and commercial actors. They are also the ones who can come up with technology solutions. Establishing close collaboration between them is a shared interest, which governments should promote.

Speaking from exactly that position, Chief Research and Strategy Officer at Microsoft Craig Mundie, spoke of some radical "home-truths" of the new cyber threat environment. "What defence agencies in the US and NATO are coming to understand is that the speed of a cyber-attack, and the scale, is a force of magnitude faster and larger in effect than any classical mode of conflict."

Faced with this unprecedented pace of attack, Mundie was unequivocal. "Active defence is going to have to occur without people in the loop….we need to think about the design of computers to which we will entrust active counter-measures, without awaiting further authorisation from people."

"*The speed and scale of a cyber-attack is a force of magnitude faster and larger in effect than any classical mode of conflict*."

Craig Mundie

This "will require a level of trust in computer systems people will not be very comfortable with," he added, but that is the price we must pay to catch up with the breakneck speed of ICT.

Mundie also railed against out-dated intellectual and legal concepts that hold back a robust response to cyber-threats. "We have trans-sovereign threats which we have retro-fitted to laws framed in terms of sovereign boundaries," he lamented. Such laws "need updating to be effective."

Harry van Dorenmalen, Chairman of IBM Europe, pointed out that time is not all we are out of – we are also out of money. "We all know we don't have enough money to fix these problems in today's climate, so we have to find smart and intelligent solutions," he explained.

To the industry representative, such solutions should focus pragmatically on best practices across Europe. "We really need to look at countries and companies that have solutions, that show leadership, and learn from them."

To facilitate this, van Dorenmalen recalled an initiative launched in The Netherlands, where a multi-sectoral cyber-security council was formed to help share points of view. "The interesting thing is, that coming from the private sector, I hear things I have not heard before," the representative remarked.

"*We need to look at countries and companies that have solutions, that show leadership, and learn from them*."

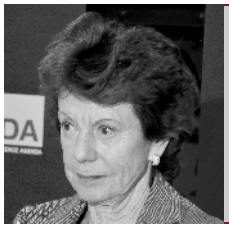
Harry van Dorenmalen

In a frank speech, van Dorenmalen demanded that we ask ourselves some fundamental questions when looking for effective solutions - even if they are abroad. "Is this working in the UK, or the Netherlands? If yes, we should take this and use it widely," he opined. Above all, "we need a plan, an approach – there is no more time."

But does Europe have a plan? Vice President Kroes believes it does, when outlining her priorities in this important policy area. "I want public and private stakeholders to exchange information on attacks and incidents," because "the credibility of cyber-security in Europe relies on the delivery of reports."

The Commissioner outlined how the EU was also stepping up collaboration with global partners, including a conference to be held this September with the US Department of Homeland Security. Such cooperation means that "we can deal with attacks, even when they are across borders", she explained.

To support such efforts, the Commissioner avowed that the EU could be willing to contribute research funding and expertise to drive innovation. "We will give industry the opportunity to test new security technology in real life scenarios, including demonstrations."



"*We must invest in security technologies and innovation at all sectors and all levels. We need to safeguard the security of the citizen*."

Neelie Kroes

To back this up, the Commissioner re-affirmed the EU's commitment to a robust budget in these areas. "We must invest in security technologies and innovation" at "all sectors, all levels – we need to safeguard the security of the citizen."

Such strong assertions are all well and good, but with the dangerous realities of the ongoing financial crisis, just how high should cyber-security really be on a European state's list of budgetary priorities?

This point was taken up by the SDA's Senior Manager, Pauline Massart, who pointed out that 63% of experts surveyed in the recent SDA cyber-security report believed cyber-security budgets should be protected from further cuts. "Are we in fact investing enough?"

Iklódy agreed that the different member states of NATO were coming to some widely diverging conclusions in this area. "The problem is the cyber landscape is extremely varied…some [allies] are advanced, with considerable capabilities, considerable preparedness - there are others where this is not the case."

Nonetheless, the ASG affirmed that NATO had the tools and mechanisms to help level out this disparity. "We are trying to integrate cyber-defence into the NATO defence planning process. This is a fantastic instrument to encourage increased spending."

Van Dorenmaelen took a different track, and instead focused on optimising the resources already allocated to this area. As well as increasing efficiencies, the IBM representative also raised a controversial idea - that it may be time to start disconnecting certain networks, rather than making more.

"It is amazing sometimes how many bodies, entities and people are connected – but some bring value, and some do not. Don't waste time and money," he warned.

Reinhard Priebe, Director for Internal Security at the Commission's DG Home Affairs, also agreed that coordinating what is already spent is a viable solution. The EU hopes to help with this, through the establishment of new agencies to support member state efforts. The European Cybercrime Centre, to be established in the coming years, is a classic example of this effort.

"Our approach is not so much to legislate, it is to exchange best practices, while bearing in mind that within the 27 club, some are more advanced," he explained. However, the official was clear that the EU would not take the lead. "There is a big community of people dealing with this at many

different levels....we expect many answers from elsewhere."

However, some fundamentally challenged the premise that cyber-security needs to be prioritised so highly. Former UK Deputy Permanent Representative to NATO Paul Flaherty suggested a "very unpalatable" idea - that existing structures of physical deterrence will largely shield us from the worst a cyber-adversary would dare unleash.

Much like the overwhelming US military response to unconventional terrorist attacks after 9/11, Flaherty proposed that a large scale cyber-attack would risk an unbearable physical response. As few would be foolhardy enough to accept the weight of that response, perhaps cyber-security is not such an overwhelming priority?

However, Microsoft's Craig Mundie disagreed with this inherently reactive policy. "You'd have to wait for an attack to run its course first", before you could respond, with all the potential damage that would entail. "That's not ideal", he noted bluntly.

Speaking from the experience of a nation that has had to "pick up the pieces" of a large-scale cyber-attack, Senior Advisor of the Estonian Undersecretary of Defence, Heli Tiirmaa-Klaar, weighed in.

In the aftermath of the 2007 distributed denial of service attack in Estonia , she claimed that one thing had become clear - "you must define what is absolutely critical" before you invest money into counter-measures. For her, this involves a survey of energy, transport, finance and other sectoral infrastructures, to identify which is fundamental to the operation of the state.

Once identified, only targeted investment will work. "Identify what is critical, and then what services that critical infrastructure relies on to function." Once you have found these underlying elements in need of reinforcement, "put your money there, to really deal with your cyber-vulnerabilities."

Yet such processes take time. Given the imperative of time expressed by all who spoke during this evening's discussion, it is clear that the cyber-security clock is ticking.

List of participants

Frank Asbeck
Principal Counsellor for Security and Space Policy
European External Action Service (EEAS)

Martin Borrett
Director
IBM Institute for Advanced Security

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

Dumitru Sorin Ducaru
Ambassador
Delegation of Romania to NATO

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

Paul Flaherty
Former Deputy Permanent Representative of the UK to NATO

Brigid Grauman
Independent journalist

Gábor Iklódy
Assistant Secretary General for Emerging Security Challenges
North Atlantic Treaty Organisation (NATO)

Thibaut Kleiner
Member of VP Neeile Kroes' Cabinet
European Commission

Neelie Kroes
Vice President & Commissioner for Digital Agenda
European Commission

Pauline Massart
Senior Manager
Security & Defence Agenda (SDA)

Giles Merritt
Director
Security & Defence Agenda (SDA)

Grigol Mgaloblishvili
Ambassador
Mission of Georgia to NATO

Jeffrey A. Moss
Vice President and Chief Security Officer
Internet Corporation for Assigned Names and Numbers (ICANN)

Craig J. Mundie
Chief Research and Strategy Officer
Microsoft

Reinhard Priebe
Director, Internal Security
European Commission
Directorate General for Home Affairs

Rene Roersma
Director Global Public Sector
McAfee

Raj Samani
Vice President and Chief Technical Officer
McAfee

Andrea Servida
Deputy Head of Unit, Internet; Network and Information Security and Commission representative to ENISA
European Commission
Directorate General for Information Society and Media

Brooks Tigner
EU/NATO Affairs Correspondent
Jane's Defence Weekly

Heli Tiirmaa-Klaar
Cyber Defence Policy Advisor
North Atlantic Treaty Organization (NATO)
Cyber Defence Section, Emerging Security Challenges Division

List of participants

Harry van Dorenmalen
Chairman, Europe
IBM Corporation

John Vassallo
Vice President EU Affairs & Associate General Counsel
Microsoft

Paolo Venturoni
Vice President European and NATO Affairs
Finmeccanica

Sal Viveros
Senior Director, Worldwide Enterprise PR
McAfee

Florian Walther
Hacker and Penetration Tester
CureSec

Annemarie Zielstra
Director
Centre for Protection of the National Infrastructure (CPNI.NL)

Upcoming cyber-initiative events

International cooperation in cyber-security

Cyber-protection of critical infrastructure

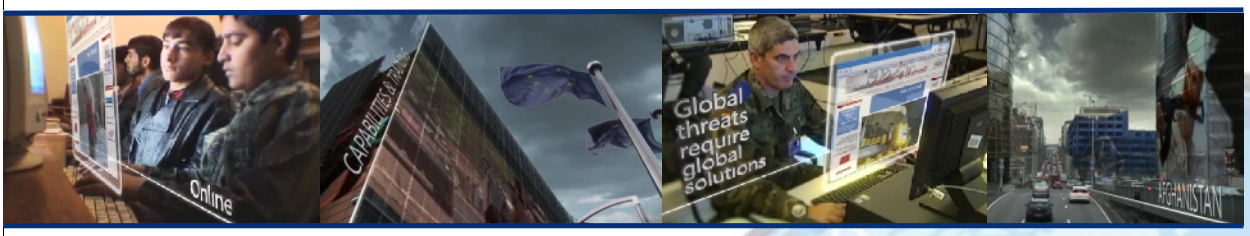
Security Jam

Brainstorming global security

19 - 23 March 2012

A 4-DAY ONLINE DISCUSSION

The Security Jam is a unique opportunity to share your views with thousands of policy-makers and experts from all over the world on pressing security & defence issues in discussions be moderated by senior experts from leading think tanks.



VIPs will include:

Admiral James Stavridis
NATO Supreme Allied Commander Europe

Claude-France Arnould
EDA Chief Executive

Vice Admiral C.A Johnstone-Burt OBE
NATO ACT Chief of Staff

Rob Wainwright
EUROPOL Director

Lt. Gen. Ton van Osch
EU Military Staff
Director General

— FUTURE CAPABILITIES — INTERNATIONAL COOPERATION
— FORGING STRATEGIC PARTNERSHIPS — CRISIS MANAGEMENT
— THE CYBER-CHALLENGE — TRANSNATIONAL & HYBRID THREATS
— LESSONS OF LIBYA & AFGHANISTAN

The most innovative recommendations will be presented to NATO and EU leaders ahead of the May 2012 Chicago summits and a full report will be presented at the SDA's international NATO conference later that month.

REGISTER AT

www.securityjam.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
@secdefagenda