SECURITY & DEFENCE AGENDA

What next for European cyber-security?

Report

March 2013

A **Security & Defence Agenda** Report
Publisher: **Geert Cami**
Project Manager: **Andrea Ghianda**
Rapporteur: **Seán Smith**
Photos: **Benoit Chattaway**
Date of publication: **March 2013**

Contents

What next for European cyber- security……2

Private-public cooperation……..2

International cooperation……...5

Skills……..8

Programme……..10

Speakers & moderator……..11

Participants……13

Upcoming events……14

Past cyber- initiative speakers & topics……..14

What next for European cyber-security?

Referring to the EU's recently published cyber-security proposals, SDA Director **Giles Merritt** began by asking "how well is the strategy going through the mincer? Do we have the right mix of legislation and non-legislative measures?"

Paul Timmers, Director of Sustainable and Secure Society, Directorate General for Communication Networks, Content and Technology, European Commission, stated that since the EU's strategy is ambitious and wide-ranging, it is important to be able to prioritise within the strategy. Should the EU be focusing more on improving resilience, tackling cybercrime, or enhancing international cooperation? Should there be greater emphasis on civil-military exercises, public-private partnerships, or network and information security platforms?

Private-public cooperation

Timmers noted that one of the guiding principles of the Commission had been to construct a Directive that is neither overly prescriptive, nor imposes excessive obligations on the private sector. "Hopefully it will simplify life rather than complicate it for the private sector - which is not self-evident", he added. "Legislation can never work without voluntary cooperation, action and flexibility from member states", which is why the Commission opted for a directive rather than a regulatory approach, he explained. Since it is a minimum harmonisation directive, member states can go further than the stated requirements if they wish. The flexibility of such 'smart legislation' is key to its success as it provides an incentive to create a level playing field without imposing too heavily on nations.

"Hopefully it [the directive] will simplify life rather than complicate it, which is not self-evident… Legislation can never work without voluntary cooperation, action and flexibility from member states."

Paul Timmers

Annemarie Zielstra, Strategic Advisor Department Cyber Security of the Dutch National Coordinator for Security and Counterterrorism (NCTV), questioned whether the EU's strategy placed sufficient emphasis on improving public-private cooperation in the cyber domain. In her view, it remains "unclear whether the strategy fosters public-private cooperation at the operation level", as well as enhancing the technical cooperation of CERT

communities.
On the issue of how legislators should interact with the private sector, Zielstra stressed that the EU ought to set the agenda by defining roles and clearly delineating responsibilities between private and public organisations. She cautioned though that agreements "cannot only be voluntary" and highlighted the need for more stringent requirements on companies producing and marketing IT security software to ensure that certain standards are met.

However, she underlined the importance of adopting strategies that contain distinct benefits for private firms to guarantee their participation, remarking that "if you have added value, they will show up for the meeting - you don't have to regulate". But more in general, there must be added value for all parties involved.

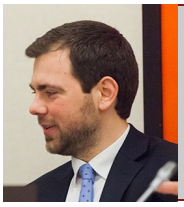
Industry leaders echoed this sentiment, with IBM's **Leendert van Bochoven** drawing on an example from the US to illustrate the point. He related how many American companies are walking away from initiatives that started out promisingly simply because "there's no value coming back". In essence, collaborative efforts have to remain beneficial to keep the business community engaged. Van Bochoven detailed the companies' complaints about how "information was coming back too slowly" or how companies were providing the authorities with information, only for it to be classified immediately thereby making it almost impossible to get back. This "one-way traffic of information" means that "industry's incentive to participate evaporates".

Troels Oerting, Head of the European Cybercrime Centre, acknowledged the problem exists on this side of the Atlantic too, outlining his daily reality concerning information sharing. "I can receive everything but I have big difficulties giving you anything back", he said. "I am a part of Europol. I'm not allowed to receive an IP address from a private company in the EU. This is my legal framework. Is this clever thinking or do we need a different approach?" On this matter, Timmers noted the EU approach does differ from that of the US, in that certain public authorities in the United States are obliged to give information to the private sector, which is not the case in Europe. Whether those authorities are performing the task well

"I am a part of Europol. I'm not allowed to receive an IP address from a private company in the EU. This is my legal framework. Do we need a different approach?"

Troels Oerting

enough to satisfy the private sector is debatable. Nevertheless, the distinction is clear: whereas information sharing remains a 'one-way street' in Europe, in the US steps have already been taken to ensure that information can flow in two directions.
Another point of contention for the private sector that emerged from the debate is the setting of standards, mentioned in Article 16 of the EU's Directive. Huawei's **Wout Van Wijk** was quite clear on the matter: "Standardisation should be international, full-stop. Almost everyone in industry agrees on that." Van Bochoven was similarly unambiguous arguing that "standards have to be set at a global level… we should avoid any European setting of standards". He emphasised the important role of large companies such as IBM in monitoring and protecting vital national services, without which any society would struggle to survive. "We are at the forefront, we are managing infrastructures. On a daily basis we are filtering 13 billion events to see what's happening." As such, the challenge for governments and regulators is "to define the incentive models" so that "we can find the joint incentives to collaborate".



"Standardisation should be international, full-stop. Almost all people within industry agree on that."

Wout Van Wijk

Timmers countered by stating that "most of the standards in the field are industry-driven". Moreover, the standards referred to in Article 16 of the directive relate to risk management and are there to assist companies, he maintained. "I think the idea that the public sector is imposing something on private sector is overdone – that's not the way it works."

Zielstra raised a separate concern, building on her comments regarding the perceived operational-technical divide in the Commission's strategy: "What we need is to close the gap between the political and operational agenda. What we agree politically will not always be resolved operationally." She also added her fear that some "organisations are becoming

"What we need is to close the gap between the political and operational agenda. What we agree politically will not always be resolved operationally."

Annemarie Zielstra

too big to build trust to share information". According to her, "trust, value and commitment" are the three principal elements for any successful collaboration.

Oerting lamented that doubts over trust and value afflict the law enforcement sector as well making his task of catching cyber criminals even more difficult: "Right now it's a free-ride to be a cyber-criminal. The number that we actually catch is relatively low. Most of the crime is committed and we do not even hear about it in the police. Banks just pay, everybody pays and nobody wants to report the crime: either because the police are incompetent or companies fear it will leak to the press." The lack of an effective reporting system is not just a problem for businesses, but also for citizens. Oerting sketched a scenario in which his mother's credit card details are stolen online. "She goes to the Danish

police and all they say is 'go to your credit company, we cannot do anything'. This destroys trust." Unfortunately, up until now "the police has been very arrogant" according to Oerting, despite the fact that 90% of critical infrastructure protection is the responsibility of private firms. He expressed his anxiety with the level of protection some large enterprises have: "Many accounting companies and law firms have a lot of digital knowledge, but very low security. They might have a firewall and two passwords – and that's it." In addition, the growth of new technologies occasionally produces more problems than it solves. "If you look at the smartphone market, there is no security by design. There is no regulation or approval of the security of apps. Yet, they proliferate."

International cooperation

Timmers brought the second important cooperational sphere to the fore, commenting that in all these areas "we are talking about solutions that also need to work internationally". Merritt asked whether the EU was best placed to lead on fostering international agreements given its inherent familiarity with having to achieve consensus internally.

Outlining the necessity for more effective cooperation amongst European nations, Timmers explained the rationale behind the EU strategy: the directive strives for a joint approach that raises capabilities, addresses risk management at the EU and national levels, and establishes mechanisms for member states to alert each other in case of a serious cyber-attack. In other words, "if you want to have a coordinated reaction by member states, you have to put national capabilities to joint use".

Addressing a question about possible international tensions and contradictions, Timmers said that there was no general answer: each sector must be analysed separately. For instance, on smart grids and cyber-security there is already very active international cooperation, which must of course continue. On the other hand, while the energy sector is beginning to think more internationally about the cyber-protection of their infrastructure, more progress needs to be made, he concluded. His verdict on how different sectors are undertaking collective risk assessments was similarly forthright: "Is there enough cross-sector collaboration? I think not."

"If you want to have a coordinated reaction by member states, you have to put national capabilities to joint use."

Paul Timmers

Zielstra questioned whether the EU was providing enough clarity to bring about a coherent approach. "The EU cyber-security strategy doesn't define all of the terms used in the Directive. It only defines a limited number", she said, arguing that clear and agreed definitions are the foundations of any successful partnership. She added that the Netherlands "would like to see more coordination of collaboration. We need the same level of cyber-security in different member states." She advocated that if member states were to prioritise their agendas collectively, such measures would help close the gap between the

political and operational agendas. It is not enough to have information sharing mechanisms between CERTs, but existing platforms must be used to promote these practices between national governments.

Oerting spelled out the problem in different terms: "Cybercrime has no borders, it can be committed from anywhere against anywhere" rendering customary crime-fighting techniques impotent. Furthermore, "the EU loses €1.5 billion every year due to online credit card fraud and €106 billion every year in VAT fraud, 65% of which is done via computers." Yet, the majority of cybercrime originates outside of the EU according to Oerting, making it essential that the EU works with foreign states. He announced that Europol is currently seeking agreements with Ukraine and Russia "to help catch crooks", but he remained somewhat sceptical towards the extent of genuine cooperation with countries like Russia and China, which "do not always share our values".

"The EU loses €1.5 billion every year due to online credit card fraud and €106 billion every year in VAT fraud, 65% of which is done via computers."

Troels Oerting

Zielstra reminded everyone of the desirability of striking such bilateral or international agreements in a globalised world: "Outsourcing means we have to collaborate with countries such as India to ensure our security."

Oerting went on to explain how cybercrime already poses problems for police forces and how the advent of cloud computing could aggravate the situation. To secure a prosecution, law enforcement forces "have to obtain evidence to make the attribution between the crime and the criminal". With data currently stored on internet servers it is possible for police to seize the servers for analysis. However, "in the future, as we move from servers to cloud computing, it will become even more difficult to gather evidence since we cannot seize the cloud if we don't even know where it is." He raised the spectre of intelligent criminals using clouds from distant, "bullet-proof countries" with which the EU and the US have no international agreements to launch their criminal activities.

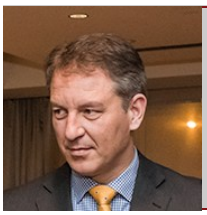
Sorin Dumitru Ducaru, Romanian Ambassador to NATO, endorsed the tough message calling for "a cyber social contract with a strong framework to punish those who abuse the domain". He bemoaned that "we have still not reached the end of the philosophical phase"

regarding cyber-security and that there are still too many "kumbaya people" maintaining a "Woodstock attitude of complete freedom" online, ignorant of the scale and prevalence of cyber threats. **Antonio de Palmas** of Boeing countered that the EU's delivery was a "tangible strategy taking shape, beyond the philosophical stage".

Bringing the discussion back to the topic of international cooperation, Ducaru asked Timmers two questions: "What can the EU do to develop a coherent approach between the EU, UN and NATO to establish an international regulatory framework? And what are the commonalities and differences between cyber approaches in the US and in the EU?" Merritt followed by asking whether we need an international body, a so-called neutral referee, such as the International Telecommunication Union, to arbitrate on cyber agreements?

Timmers replied that the US and the EU enjoy a lot of common ground. Both are pursuing risk-based approaches and would have only minor problems to overcome in agreeing an international rule book. Whilst it may look to the outside world that the US wants to regulate less, this is not really the case according to Timmers, as the proposed legislation in the US would contain legal requirements not too dissimilar to those in the EU's directive. In answer to Merritt's question "Would it help you to have something in Geneva?", Timmers said that establishing such a body was not on his list of priorities. Moreover, he pointed to the fundamental strategic difference between the EU and an organisation like NATO that refers to 'cyber-defence'. When it comes to cyber-security "the EU doesn't talk about warfare – we don't have the defence element at all", adding that the EU is focused on building competencies through international cooperation.

Van Bochoven intervened to suggest that the development of strategic early warning systems would be a fertile breeding ground for EU-NATO cooperation, given the rise in state-sponsored cyber-attacks. As for military-led cyber exercises, he championed the role the private sector could play. "Too often we see cyber-defence exercises on the military side with no real private sector involvement", he said. Instead, we need to "find ways to do such exercises together as joint exercises with industry involvement are crucial" to making our cyber defences more resilient.



"Too often we see cyber-defence exercises on the military side with no real private sector involvement", he said. Instead, we need to "find ways to do such exercises together as joint exercises with industry involvement are crucial."

Leendert van Bochoven

Skills

Skills are the one area where many commentators feel the EU's proposals are lacking. **Heli Tirma-Klaar,** from the European External Action Service, led the way. "The EU strategy missed out on skills; there should be more emphasis on training. However, it is not too late: we can still make additions." In her opinion, global agreement on the subject is still "20 to 30 years away" because "we are not dealing with like-minded partners". It is therefore imperative to prioritise things the EU can achieve, such as raising awareness and education. She outlined some of the deficiencies in need of correction. One, the costs of cyber-security remain high because the market supply of skills is limited. The cost of technology itself is not high, but the cost of knowledge is. Boosting the supply pool of cyber skills will cause knowledge costs to fall. Two, "very few people in the EU can grasp the defence and security element of the cyber phenomenon". And three, "we do not currently have a good intelligence system in the EU to always be able to feed Troels and Europol the information they require". Education is the key to tackling these inadequacies, she proposed. "Now is the time to have the intellectual clarity to decide what should be done at different levels", she stated.

"We do not currently have a good intelligence system in the EU to always be able to feed Europol the information they require."

Heli Tirma-Klaar

Oerting reinforced the call for more ambitious educational programmes, claiming that: "my children spend 80% of their waking time on social media and on the internet, yet they have never received one minute of education at school about how to act, react and interact online. They simply don't know. They have to learn this by doing. Is this good? No."

On a more positive note, he highlighted that the University of Leiden in the Netherlands is in the process of establishing a cyber academy in cooperation with Europol to produce the next generation of cyber professionals. A university in Germany has also agreed to set up a similar academy, remarked Oerting. "We need the skills to attack the criminals", he urged.

Timmers recognised that the initial feedback from member states has been that "we did not emphasise the skills side enough in the cyber-security strategy", although he did remind participants of existing awareness-raising activities, such as the EU's upcoming cyber-security month in October 2013.

Zielstra said that efforts must also include risk management skills, as the problem cannot be confined to the IT department but involves other departments, such as Legal (intellectual property, liability), Communications (awareness, reputation, crisis communications), Finance (risk management, insurance), Procurement and last but not least Operations, where things really happen. She underlined that educational programmes cannot neglect training on security skills and that we must encourage "not only awareness, but behavioral change".

Merritt concluded that “we’re a long way from a common threat analysis, even in Brussels. We need to try and establish more objectively where cyber-security and critical infrastructure protection fit together with the cybercrime approach.” Furthermore, we need to start be more professional about risk analysis, he urged. The advent of the cyber problem has coincided with the economic downturn, making the issue of money unavoidable. “What sort of costs are we looking at? In the EU, should we be looking at sharing of costs between rich and poor? We already do it in other areas, so why not in the cyber domain?” he asked. Finally, he returned to one of the central elements of the discussion, contending that it is not only cheaper to train and educate people at an early age, but that it is far more effective to instil lessons in children rather than trying to graft skills onto them in later life.

Programme

With the recent publication of the European Commission's cyber-security strategy and the opening of the European Cybercrime Centre, what further advances can be hoped for in European cyber-security in 2013? How are stakeholders judging the Commission's proposal? Can the new Cybercrime Centre coordinate national Computer Emergency Response Teams (CERTs), and how can the EU ensure that it has the right skills? Will the new European strategy improve public-private cooperation in cyber-security? To what extent could the Commission's proposals be the first step towards a more global approach to regulation on cyber-security? Is the new strategy likely to strengthen cooperation and information exchange beyond the EU's borders?

Speakers:

Paul Timmers, Director, Sustainable & Secure Society, European Commission
Troels Oerting, Director, EU Cybercrime Centre
Annemarie Zielstra, Strategic Advisor Department Cyber Security of the National Coordinator for Security and Counterterrorism (NCTV), Ministry of Security and Justice, The Netherlands

Moderated by **Giles Merritt**, Director of the Security & Defence Agenda

Speakers & moderator

Troels Oerting
Head of the European Cyber Crime Centre (EC3)
European Police Office (Europol)

Troels Oerting is Head of the European Cyber Crime Centre (EC3), which opened in January 2013. He is also Assistant Director of Europol's Operations Department and Information Management and Technology (ITM).

Before joining Europol, he was Director of Operations in the Danish Security Intelligence Service, Director of the Danish Serious Organised Crime Agency (SOCA), and Director of the Danish National Criminal Intelligence Service (NCIS). Prior to this, he worked as a Detective Chief Superintendent responsible for combatting national and international cases of organised crime, financial crime, fraud, tax evasion, money laundering and corruption.

Oerting also led Europol's delegations to Southeast European Cooperation Initiative (SECI), Interpol, the Maritime Analysis and Operations Centre (MAOC), the Baltic Sea TaskForce, the Committee Article Thirty-Six (CATS), the Committee on Internal Security (COSI) and the Counter-Terrorism Working Group (CTWG).

Paul Timmers
Director, Sustainable & Secure Society
Directorate General for Communication Networks,
Content and Technology, European Commission

Paul Timmers is Director of the Sustainable & Secure Society Directorate in the European Commission Communications Networks, Content and Technologies Directorate General (DG CONNECT).

Previously he headed the ICT for Inclusion and the e-Government unit (EU policy, research and promotion). He was a member of the Cabinet of former European Commissioner Erkki Liikanen (Enterprise and Information Society) where he was responsible for the information society and telecommunications policy portfolios. Other activities in the European Commission have included electronic commerce policy and programme development.

Timmers has also been a manager in product marketing and head of software development in a large IT company and co-founded a software start-up. He holds a PhD in theoretical physics from the University of Nijmegen, the Netherlands and an MBA from Warwick Business School, UK. He was awarded an EU Research Fellowship at the University of North Carolina in Chapel Hill, USA in 2009. His works in the field of technology and policy have been widely published, including a book on electronic commerce strategies and business models, and has been a visiting professor and lecturer at several universities and business schools across the world.

Speakers & moderator

Annemarie Zielstra
Strategic Advisor Department Cyber Security of the National Coordinator for Security and Counterterrorism (NCTV)
Ministry of Security and Justice, The Netherlands

Annemarie Zielstra is currently working as Strategic Advisor for the Dutch Department of Cyber Security. She has been working in the cyber security field since 2006.

Since 2006 Zielstra has been working within the Dutch government to help protect critical national infrastructure. From 2006-2010 as programme manager NICC (National Infrastructure against Cyber Crime) and from 2010-2012 as director CPNI.NL (Dutch Centre for Protection of the National Infrastructure). Zielstra was during this period responsible for setting up a national infrastructure for public private information sharing. Since 2013 she has been working as director International Relations on Cyber Resilience for TNO.

Zielstra is also responsible for the National Roadmap to secure Process Control Systems, chair of the EuroSCSIE (European SCADA and Control Systems Information Exchange) and coordinator of ERNCIP's (European Reference Network on Critical Infrastructure Protection) Thematic Group on Industrial Control Systems and Smart Grids, a project of the European Commission/Joint Research Centre (2012-2014).

Giles Merritt
Director
Security & Defence Agenda

Giles Merritt is the Director of the Security & Defence Agenda (SDA), the only Brussels-based security and defence think-tank.

A former Brussels Correspondent of the Financial Times (FT), Giles Merritt is a journalist, author and broadcaster who has specialised in the study and analysis of public policy issues since 1978. He was named one of the 30 most influential 'Eurostars' by the Financial Times.

Merritt is also head of the SDA's sister think-tank *Friends of Europe*, whose debates and reports cover the whole spectrum of non-defence topics, and Editor-in-Chief of the policy journal *Europe's World*. Published three times a year, *Europe's World* is the only pan-European publication that offers policymakers and opinion-formers across Europe a platform for presenting ideas and forging consensus on key issues. It is published in partnership with a coalition of over 150 think-tanks and universities worldwide, and has a readership of 120,000 senior decision-makers and opinion-formers.

Merritt joined the Financial Times in 1968. From 1972 he was successively FT correspondent in Paris, Dublin, Belfast, and Brussels, until leaving the newspaper in 1983. Since 1984 he has been a columnist for the *International Herald Tribune* (IHT), and his articles on its editorial page span a broad range of EU political and economic issues.

Participants

Dragos Basmaluta
Chief Executive Officer
Mira Telecom

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

Antonio De Palmas
President EU & NATO Relations
Boeing

Eva Diaz Perez
VP Head of NATO/EU Sales & Political Affairs
Cassidian

Sorin Dumitru Ducaru
Ambassador
Delegation of Romania to NATO

Andrea Ghianda
Project Manager
Security & Defence Agenda (SDA)

Brigid Grauman
Independent journalist

Wilfried Grommen
Director & CTO
Hewlett Packard

Demosthenes Ikonomou
Head of Secure Services & Project Support Activities
European Network and Information Security Agency (ENISA)

David Luengo
Head of Brussels Office
International Directorate
Indra

Friedl Maertens
European Union Business Development Executive
IBM Belgium

Pauline Massart
Senior Manager
Security & Defence Agenda (SDA)

Giles Merritt
Director
Security & Defence Agenda (SDA)

Roy Nitze
Second Secretary
Permanent Representation of Germany to the EU

Troels Oerting
Head of European Cybercrime Centre
European Police Office (Europol)

Jeffrey Rogers
Business Development Executive
Raytheon Systems

Nagayo Taniguchi
Journalist
Sentaku/SEKAI

Paul Timmers
Director, Sustainable & Secure Society
Directorate General for Communication Networks, Content and Technology
European Commission

Heli Tirma-Klaar
Cyber Security Policy Advisor
European External Action Service (EEAS)

Leendert van Bochoven
NATO and European Defence Leader
IBM Europe

Wout Van Wijk
EU Public Affairs Manager
Huawei Technologies

Wim Wensink
Principal Manager
PricewaterhouseCoopers

Katerina Wright
Senior Analyst
The Avascent Group

Annemarie Zielstra
National Coordinator for Counter-terrorism and Security; Strategic Advisor, Cyber Security Department
Ministry of Security and Justice, The Netherlands

Upcoming events

Cyber-initiative

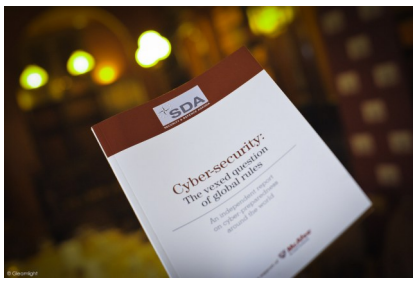
The initiative will build on the experiences and debates of 2011 and 2012, digging deeper into the issues and expanding into new areas.

It will seek to examine global governance matters such as the application of international law on cyber-space, EU-US cooperation, as well as building confidence and trust between different stakeholders. The initiative will analyse horizontal policy issues such as resilience, skills, training and education.

Past cyber-initiative speakers & topics

The 2012 saw the first year of the SDA's cyber-security initiative, which concentrated on defining cyber-security and the most prominent threats, as well as the interactions between the private and public sectors.
The evening and dinner debates evolved around topics such as international responsibility, information and intelligence sharing, prevention and resilience, cyber-preparedness in EU states and legislative proposal of the EU, protection of critical infrastructure as well as public-private partnerships.

SDA's 2011-2012 cyber-initiative debates have welcomed: **Gabor Iklody**, NATO Assistant Secretary General for Emerging Security Challenges, **Neelie Kroes**, Vice President & Commissioner for the Digital Agenda, European Commission, **Cecilia Malmström**, EU Home Affairs Commissioner, **Jeff Moss**, Vice President & Chief Security Officer, Internet Corporation for Assigned Names and Numbers (ICANN), **Troels Oerting**, Assistant Director of Operations, European Police Office (EUROPOL), **Chris M.E. Painter**, Coordinator for Cyber Issues, United States Department of State and Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges, NATO.



In 2012, the SDA also launched its groundbreaking cyber-report "*Cyber-security: The vexed question of global rules*", based on over 80 interviews with senior specialists and policy makers and a survey of 250 experts from around the world.

The report can be downloaded at
www.securitydefenceagenda.org.

SECURITY & DEFENCE AGENDA (SDA)

4 Rue de la Science
1000 Brussels, Belgium
Tel: +32 (0)2 300 29 92 **Fax**: +32 (0)2 300 29 90
E-mail: info@securitydefenceagenda.org

www.securitydefenceagenda.org
Follow us on twitter @secdefagenda