Cyber-security:

Problems outpace solutions

Annual report

SECURITY & DEFENCE AGENDA

Disclaimer

The views expressed in this report are the personal opinions of individuals and do not necessarily represent the views of the Security & Defence Agenda, its members or partners.

Reproduction of this report, 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 reproduction, whether in full or in part, is not sold unless incorporated in other works.

All job titles given refer to positions held at the time of publication.

A ***Security & Defence Agenda*** report

Publisher: **Geert Cami**

Project Manager: **Pauline Massart**

Project Assistant: **Paul Cohen**

Date of publication: **December 2013**

Pictures: **© Security & Defence Agenda**

SECURITY & DEFENCE AGENDA
4 Rue de la Science,
1000 Brussels, Belgium
T: +32 (0)2 300 29 92 F: +32 (0)2 300 29 90
E: info@securitydefenceagenda.org
W: www.securitydefenceagenda.org

Follow us on Twitter @secdefagenda

Contents

Foreword

Why we must deepen the cyber-debate while raising its profile

Giles Merritt
Chairman
Security & Defence Agenda

A former Brussels correspondent of the Financial Times, 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. He is also Editor-in-Chief of the policy journal Europe's World*, and Secretary General of the SDA's sister think-tank Friends of Europe.*

The SDA's cyber-security debates during 2013 saw stakeholders agree on the urgent need to enhance cyber-security awareness and education. Awareness is crucial to further development since the weakest links in the chain are the users, be they individuals, companies or governments while education is decisive in mitigating the shortage of skilled cyber-professionals.

Edward Snowden's disclosures have been a serious blow to citizens' trust of governments. Can political leaders still impact users' online behaviour? Is personal data gathering an infringement of human rights or a "necessary evil"? How can governments be held more accountable in cyber-space? Cyber-security's concepts and legislation clearly need to be better defined.

Technological innovation is fast moving, so governments must cooperate more effectively if they are to keep up, not only by sharing information but also by clearly defining the tasks of institutions and national authorities: what should an ideal division of labour between NATO, the EU and their member states look like?

The wide variety of cyber-security stakeholders should lead in both the public and the private sectors. But we must beware of blanket solutions: combating cyber-crime is different to protecting organisations' networks and cyber-espionage demands different responses than cyber-attacks. Cooperation also means closer public-private collaboration, including with the myriad innovative SMEs entering the field. Innovation may come from the private sector but priorities are set by political decision-makers, as when President Barack Obama issued an executive order on cyber-security in February identifying cyber-insurance as a necessity.

In Europe, we are at a cross-road, with the EU's cyber security strategy being implemented and the Commission planning for a directive on data protection. We need clear rules and we need them soon, but rushing policy choices may mean choosing the wrong ones.

What next for European cyber-security?

Dinner debate

19 March 2013, Brussels

Moderator: Giles Merritt; Rapporteur: Seán Smith

Speakers

Troels Oerting

Head of the European Cyber Crime Centre (EC3)

European Police Office (Europol)

Troels Oerting has been Europol Assistant Director since 2009 and serves as Head of the European Cybercrime Centre (EC3) and Interim Head of Europol Counter Terrorist and Financial Intelligence Centre. He was Director of Operations in the Danish Security Intelligence Service, starting his career in the police back in 1980. He served as Director of the Danish NCIS, Director of National Crime Squad and later as Director of the Danish Serious Organized Crime Agency.

Paul Timmers

Director, Sustainable & Secure Society

European Commission Directorate General for Communication Networks

Timmers was a member of the Cabinet of former European Commissioner Erkki Liikanen 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.

Annemarie Zielstra

Strategic Advisor Department Cyber Security of the National Coordinator for Security and Counterterrorism (NCTV)

Ministry of Security and Justice, The Netherlands

Since 2006 Zielstra has been working within the Dutch government to help protect critical national infrastructure. 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.

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’

“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

is key to its success as it provides an incentive to create a level playing field without imposing too heavily on nations.

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.

> *"Standardisation should be international, full-stop. Almost all within industry agree on that."*
>
> **Wout Van Wijk**

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 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.

> *"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."*
>
> **Troels Oerting**

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".

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

“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

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 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".

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

Paul Timmers

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."

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”.

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.

“Too often we see cyber-defence exercises on the military side with no real private sector involvement, [we need to] find ways to do such exercises together as joint exercises with industry involvement are crucial”

Leendert van Bochoven

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.

Skills

> *"We do not currently have a good intelligence system in the EU to always be able to feed Europol the information they require."*
>
> **Heli Tiirma-Klaar**

Skills are the one area where many commentators feel the EU's proposals are lacking. **Heli Tiirma-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.

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.

The steps needed to protect the EU's critical infrastructure against cyber-attack

Sir David Omand is Visiting Professor at King's College, London, a former UK Security and Intelligence Co-ordinator and Permanent Secretary of the UK Home Office

Twenty years ago this article would have highlighted the 'ring of steel' put around the critical infrastructure of the City of London to keep out the Provisional IRA's bombers. Ten years ago, it would have focused on the measures taken to prevent a 9/11-style attack on European capitals by Al-Qaeda. Today, the major challenge to infrastructure, security and economic well-being comes from the threat of cyber-attack.

It is a hot topic. Last year we saw a cyber-attack on Saudi Aramco, which supplies around a tenth of the world's oil; that destroyed or compromised around 30,000 computers and 2,000 servers. In that same month, cyber-attackers crippled Qatar's RasGas natural-gas company email and other administrative systems. Both attacks are believed to have been by Iran, although it is notoriously difficult to provide courtroom evidence as to where an attack originates – although inferences can be drawn from secret intelligence.

The ability to conduct cyber-sabotage against critical infrastructure exists, and will increase, and both the U.S. and Europe are playing catch up. The Washington Post earlier this year leaked the top secret U.S. Presidential Policy Directive 20, which calls on America's national security leaders to develop destructive cyber-warfare capabilities that "can offer unique and unconventional opportunities to advance U.S. national objectives around the world, with potential effects ranging from the subtle to the severely damaging." The UK (and no doubt other major European powers) is now investing resources in understanding these technologies.

We must not expect that in the future restrictive policies or sanctions can be imposed on a country – even with the weight behind them of the UN Security Council – and not expect cyber retaliation. We are currently witnessing hostile cyber reconnaissance of key critical infrastructure in the U.S. and Europe. So far these have just been exploring and probing for weaknesses, but I can confidently predict that the ability to sabotage infrastructure will improve. There is an active black market in techniques and knowledge of vulnerabilities, and proliferation of these represents a major risk for Europe.

For much of resilience planning, of course, the difference between malign threat and natural hazard is less important than mitigating the impact on society. How long until services can be restored is the principal pre-occupation. Unexpected disruptions of normal life are still more likely to come from accidents or natural hazards and disasters like earthquakes and floods than from deliberate sabotage. The most demanding scenarios are those where related risks are likely to cascade in a domino effect presenting problems that link quite different sectors. This may occur with advanced cyber-attacks; the interaction of European energy distribution and telecommunications systems being a case in point, and electricity supply and water treatment would be another. The cyber vulnerabilities of critical infrastructure are relatively uncharted territory for Europe.

"The ability to conduct cyber-sabotage against critical infrastructure exists, and will increase, and both the U.S. and Europe are playing catch up. "

The more advanced a region is in terms of its dependence on digital technologies, of course, the more vulnerable it is to cyber-attack. That is proving true right across Europe as cyber infrastructure increasingly spans borders. And our economic future in Europe depends on managing these risks down to the point where confidence is maintained. European cyberspace has to be seen as a safe enough place not just to do business, but also for the use of cyber technology to innovate and create wealth. The nightmare scenario is that cyber-crime, espionage, subversion and sabotage could cause such a loss of the confidence that the markets and indeed the general public would doubt whether they can operate safely and securely in Europe's cyberspace.

So what can be done? The UK uses security planning to assess likely losses as the product of a number of factors. First, there's the number, skill level and degree of motivation of the groups who might wish to launch an attack. Then, there is the vulnerability to attack of society, together with its networks, systems and infrastructure. Third, there's the scale of the initial impact – whether it be social, financial or reputational – when an attacker gets through our defences. Finally, there's the duration and therefore the cost of the ensuing disruption before normal services can be resumed.

These factors can be multiplied together to give the expected value of the total loss to be faced. The good news is that all four of these factors can be significantly influenced if governments and the private sector act together.

In reverse order, we can address them as follows. We can reduce the time taken to get back to normal by ensuring there is a core of capabilities in the critical information and communications infrastructure to provide the IT capability to help repair and reinstate damage in other critical infrastructure sectors such as finance.

Who is going to pay for this capability? Most of Europe's infrastructure is in the hands of the private sector, although usually in industries that are in part regulated by the state. It should therefore be a licence condition for any company operating critical systems that they must maintain such core capabilities. Regulators already have to ensure their industry complies with national, European and international safety legislation, and now we have to add cyber security to that. In that way we can ensure a level competitive playing field, and in most cases we must accept that the costs will in any case have to be passed on to the consumer.

Moving on to the next factor, we can reduce the scale of initial impact by building real time situational awareness of attacks that is shared between governments and the private sector. Government has to show it can be trusted by industry with this sensitive information. Any information about attacks and anticipated attacks has to be shared at network speed between the machines patrolling our cyber frontier, government intelligence agencies, law enforcement, the impacted private parties and other actors who need to be forewarned before they suffer the same attack.

The largest short-term impact on the risk can come from the third factor in the risk equation, reducing vulnerability. That means much more cyber security education and acceptance by business and industry of the importance of protecting information networks. Boardrooms need to recognise the commercial risks they run if they don't invest in security, including the handling of employees to minimise insider risks. And they need to ask who are the technical experts who have access to the heart of the infrastructure (the Edward Snowdens) and whether or not just one person should have the keys to the kingdom.

The biggest test of the UK's approach to reducing vulnerability came with the Olympics last year. In the 18 months before the Olympics, I chaired nine table-top exercises in the UK government's COBR situation centre, with the senior players who would be in charge on the day. The aim was to think through scenarios involving different kinds of risk to public safety, including a cyber-attack on the infrastructure. Full-scale live exercises then tested the readiness of all involved, including the games managers from the London organising committee and their volunteers, the police, local authorities, transport operators, key operators of the critical infrastructure, central government, border and immigration authorities, the Foreign Office along with the armed forces, intelligence agencies and other cyber response mechanisms. The Olympic Games passed without major incidents, cyber or otherwise, and such attempts as were made to disrupt the games and defraud the public were foiled. It is nevertheless highly likely that over the next five years one or more EU countries will face some sort of advanced cyber threats.

Finally, the likelihood of attack can be reduced by catching and prosecuting lower level hacktivists and criminals, and making their activities harder. Countering really advanced attacks, however, will depend on a combination of intelligence-led active defences that are ready to respond proportionately to an attack (but not necessarily symmetrically and not necessarily in cyberspace) coupled with the threat of using all elements of national power should there be a devastating attack. We also need to see the development of accepted international norms of behaviour, and a setting of limits for misbehaviour.

A small start has been made on this with the agreement in the UN Group of Governmental Experts on Cyber Issues that international law, especially the UN charter, applies to cyberspace. The internationally accepted laws of armed conflict, for example, aim to minimise civilian suffering when conflict occurs, and that principle applies to attacks on civilian infrastructure in the cyber realm. These are steps that need active European support. There has also been an agreement between Washington and Moscow to reduce the risk of conflict in cyberspace through real-time communications about cyber incidents of national security concern, and that approach could be extended.

For the future, we need agreed norms that reflect the fact that all advanced trading nations stand to lose from the instabilities that cyber-attacks can generate, especially those that result from nations fearing that in a major international crisis their critical military, space and national financial and other infrastructure has been compromised. All the major trading nations stand to lose from the economic damage a loss of confidence in cyberspace would lead to, not least those in Europe.

We must not expect that in the future restrictive policies or sanctions can be imposed on a country – even with the weight behind them of the UN Security Council – and not expect cyber retaliation

Regulators already have to ensure their industry complies with national, European and international safety legislation, and now we have to add cyber security to that.

SecDef is an annual high level conference co-organised by the SDA and CEIS which gather key actors from both civilian and military backgrounds to exchange ideas and discuss the future of security and defence.

EU-NATO: The search for a common cyber-strategy

International conference
19 March 2013, Brussels

Moderator: Giles Merritt, Rapporteur: Séan Smith

Speakers

Koen Gijsbers

General Manager of the Communications and Information Agency

NATO

Prior to his current position at NATO, Gijsbers worked in the Dutch Ministry of Defence, where he was responsible for coordinating the major reorganisation of the defence organisation. In 2006 he was appointed Assistant Chief of Staff for Command, Control, Communications, Computers and Intelligence (ACOS C4I) of NATO's Allied Command Transformation in Norfolk, VA, US. He moved back to the Netherlands to become responsible for IT and business management policy at the Ministry of Defence and Chief Information Officer (CIO).

Sébastien Héon

Director of Political Affairs for Cassidian Cyber Security

EADS

Héon joined Cassidian in 2009 as Senior Advisor for Intelligence & Cyberdefence. He is now in charge of developing trusted relations with national authorities and governments in the cybersecurity arena. Since 2005, he has been an associated professor at Paris 7 University, teaching cryptology and protocol security to postgraduate students.

Maciej Popowski
Deputy Secretary General
European External Action Service

Popowski is a Polish diplomat who has been working on European Union affairs since the beginning of his career. In 2009, he was seconded from the European Commission to head the cabinet of Jerzy Buzek, then President of the European Parliament. From 2008 to 2009, Popowski was a Director at the Development Directorate General of the European Commission.

Marietje Schaake
Member, Committee on Foreign Affairs
European Parliament

Schaake serves on the Committee on Foreign Affairs, where she focuses on neighbourhood policy. In the Committee on Culture, Media, Education, Youth and Sports she works on Europe's Digital Agenda and the role of culture and new media in the EU´s external actions. In the Committee on International Trade she focuses on intellectual property rights, the free flow of information and the relation between trade and foreign affairs.

Europe's sense of cyber vulnerability is growing in the wake of revelations about the extent of US and UK eavesdropping on allies, said SDA Director **Giles Merritt** as he opened the debate. But although the revelations from US intelligence whistle-blower Edward Snowden have caused tensions, the allies on both sides of the Atlantic are painfully aware of the need to boost their common defences against cyber-attack.

One key issue facing NATO is the question of a "cyber-doctrine" and most crucially whether the Alliance needs to bring cyber events under Article 5 of its founding treaty which states that an attack on one ally will be treated as an attack on all.

“If a nation asks for assistance, we can help,” said **Koen Gijsbers**, General Manager of Communications and Information Agency at NATO.

However, he acknowledged that six years after Estonia suffered a serious breach of its digital networks in 2007, Alliance experts have yet to conclude if such an attack fell would fall under the Article 5 framework. “In the case of a physical attack, the doctrine is clear; but for cyber, it remains unclear,” Gijsbers said.

A group of international experts commissioned by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in the Estonian capital drew up the so-called "Tallinn Manual" early this year which concluded that nations would be in their rights under international law to respond with conventional weapons against a cyber-attacker who caused death, destruction or damage on a significant scale. However the manual is not an official NATO document.

> *“In order to build our resilience and enhance our preparedness, our approach must be comprehensive and go beyond purely military exercises. “*
>
> **Maciej Popowski**

Pressed by Merritt and Dutch Member of the European Parliament (MEP) **Marietje Schaake** to clarify NATO’s cyber-security strategy, Gijsbers explained that defending the Alliance's own networks and infrastructure is paramount, while helping Allies protect their IT systems remains a secondary element of NATO’s work.

Sébastien Héon, Director of Political Affairs for Cassidian Cyber Security at the European Aeronautic Defence and Space Company (EADS), praised NATO’s achievements in setting up the CCDCOE and the "visionary" approach of the EU in creating the European Network and Information Security Agency (ENISA) in 2004.

However, he complained that the cyber industry in Europe needs to follow that of the United States in pushing through vertical consolidation and ending costly national divisions. “The picture is still too fragmented to be efficient,” Héon said.

In addition, Europe needs to do more to support the “incredible number of innovative start-ups and SMEs” working in the cyber field, but suffering in a market insufficiently structured to promote growth potential. “Although EU regulations do promote high-grade

security solutions," Héon warned, "there is a risk of Europe losing out without more concrete projects to stimulate innovation and competitiveness."

Maciej Popowski, Deputy Secretary General for Inter-Institutional Affairs at the European External Action Service (EEAS), also stressed the need for greater synergies between the military and civilian side, between NATO and the EU, and between the private and public sector.

"In order to build our resilience and enhance our preparedness, our approach must be comprehensive and go beyond purely military exercises," he said.

> *"In the case of a physical attack, the doctrine is clear; but for cyber, it remains unclear."*
>
> **Koen Gijsberg**

Popowski pointed out that the EU is a regular observer at NATO cyber exercises, and urged the development of more civilian-military research at the EU level. "Such synergies could help advance collective industrial and technical resources," he said.

Greater cooperation could bring synergies between NATO's military and defence work and the greater EU focus on fighting cybercrime, for example with Europol's European Cybercrime Centre (EC3) which was inaugurated early this year.

Popowski said the EU was pushing for stronger humanitarian laws in cyberspace and promoting application of the 2001 Budapest Convention against cybercrime. The EU remains committed to a multi-stakeholder approach to internet regulation, that involves both public authorities and industry, he added.

Underscoring the importance of bringing together different players to bolster cyber-defences, Gijsbers pointed to an ongoing initiative in the Netherlands involving industry, government and academic experts to find common solutions - an approach he would like to see pursued at the supranational level.

"If we could get academia, industry and institutions working together more closely, training programmes could improve simply through sharing the respective capabilities of each sector," Gijsbers said.

However, he recognized that varying national levels of technology, data protection and cyber resilience are an obstacle to greater cooperation.

To counter that problem, Popowski, said the EU aims to harmonise approaches and establish common objectives to foster greater information exchanges among member states.

He also stressed the importance of engaging with industry, pointing out that roughly 85% of cyber assets in the West are in the hands of the private sector, making cyber fundamentally different from traditional state-dominated security fields.

Underscoring the risks facing the private sector, Héon mentioned an attack his company helped defeat recently on a large multinational corporation which had been ongoing for over five years before being detected and involved over 40 malware and viruses. Businesses need to alter their entire approach, he argued, to increase defence levels and move cyber-security decisions from the IT department to the boardroom.

“When I ask the key decision-maker at a company under attack whether I should cut the internet and stop the production chain, I often receive no clear answer,” Héon said. “That is where the problem often lies: there is simply no decision-making when a crisis occurs.”

Nevertheless, he remained optimistic that the cyber-threat can be defeated and was one of several speakers who warned against cyber scaremongering.

“We need to stop scaring people with the prospect of cyber catastrophes," he said. "Life entails many risks, but we can deal with them by taking pragmatic and cost-effective measures. Risks in the cyber domain should be dealt with like any other.”

“Risks in the cyber domain should be dealt with like any other.”

Sébastien Héon

Schaake agreed on the need to “eradicate the fear and hype” surrounding cyber-threats. She complained that media reports on the extent of the danger often rely on data from IT companies with an interest in selling software.

“It may be a fine business model, but it doesn’t help advance the public discussion,” said the MEP from the Alliance of Liberals and Democrats for Europe (ALDE) group.

In the Q&A session, **Leendert van Bochoven**, NATO and European Defence Leader at IBM, denied the private sector exaggerates the risk. He said IBM’s twice-yearly XForce Trend and Risk Report uses statistics from customer networks to build awareness rather than hyping dangers.

Schaake also blamed governments for ramping up the rhetoric around cyber-security. She cited former US Defence Secretary Leon Panetta’s warning of a “cyber Pearl Harbour” as a bad example of a government seeking legitimacy for the toughest possible form of response.

Drawing a parallel with the US "war on terror," Schaake said authorities had to find a balance between security and freedom. "When we tackle these issues, it is useful to keep in mind what we seek to defend," she said.

In a reference to Snowden's revelations of widespread monitoring of private communications by US intelligence services, Schaake said "mass surveillance can never be proportionate and is in direct conflict with human rights." Instead, she advocated a society-wide exercise to build resilience and public debates on proportionate and justifiable security measures.

Quizzed by Merritt on the scale and origin of cyber-attacks, Héon said effective network monitoring could make it easy to keep track on the number of attacks.

"It is not difficult to assess, so long as we have the means of effective detection," he said, adding that most attacks can be easily dealt with.

"Day-to-day, simple measures of basic hygiene could eliminate 70-80% of the threats," Héon explained. The rest can usually be handled by experts, he said, adding however that defences could be made more effective through the creation of large databases on attack information and early detection.

Schaake and Gijsbers both suggested that the major problem is less in confronting the attacks and more in attributing their origin to enable prosecution of perpetrators.

"Mass surveillance can never be proportionate and is in direct conflict with human rights."

Marietje Schaake

The MEP also urged tighter restrictions on the international trade in IT software saying it is "scandalous" that European companies can freely export sophisticated surveillance programmes to authoritarian states.

Exported technology could also be used against European interests, Schaake warned. She complained of a "lack of appreciation of the rapid proliferation of technologies that can have an offensive capacity."

The panel also looked at the question of legally obliging victims to report cyber-attacks in order to improve the authorities' wider threat awareness.

Héon supported the idea - indicating the way private data is shared in Britain and the United States - however he felt full publication was going too far.

Gijsbers explained that NATO's would not "reveal its vulnerabilities" and thus "help the enemy." However he said it was important for security organisations and particularly Computer Emergency Response Teams (CERTs) to share technical data with each other.

Europe's World
THE ONLY EUROPE-WIDE POLICY JOURNAL

The “internet of things” holds golden promises, but also daunting cyber-threats

Urmas Reinsalu, Estonia’s Defence Minister

Imagine a world in which you get home to rooms at a pleasant temperature, where the lights switch on as you enter the front door, where coffee starts brewing the moment your morning alarm rings, and from which you never have to go out because you’ve forgotten to buy new batteries for your remote control. None of this is because you forgot the lights when leaving in the morning or because you keep a large stock of batteries at home, but because your house “knows” when to switch on heat and lights in advance, and when your batteries will run out so it can order new ones.

All these home comforts are part of what is commonly called “the internet of things”, or sometimes “machine-to-machine”. They represent a reality that was first conceptualised over 10 years ago and will be within the grasp of many of us in the not-too-distant future. The internet of things doesn’t simply mean that everyday electronic devices have been manually set on a timer to do a task or that they will send various annoying reminders. Instead, it means that they can do these basic tasks themselves, reducing unnecessary and repetitive human tasks.

All these new conveniences may be fairly minor, but they illustrate how just a tiny part of the internet of things would work. Much more important is the way the internet of things promises a smart environment that would offer immense savings of time, energy and resources. It’s a new concept that in the future entails our being surrounded by increasingly interdependent networks of smart communications, smart grids, smart homes, smart traffic, smart health and so on. The internet of things could eventually mean we not only will have smart homes or streets but entire smart cities and countries that are made more efficient by computer-based management and machine-to-machine communications. The technology that would enable this is already possible, which means that this vision is becoming more and more real by the day.

But the internet of things also brings with it new challenges. To understand how it may affect the defence sector, especially cyber-security, we have to look at defence not as a narrow field but as something that – just like the internet of things – is interconnected.

One of the hallmarks of the modern security environment is that it encompasses much more than traditional "hard" security and defence, which put the emphasis on military strength and resilience. A broader view of the changing security environment presents many other areas like energy, telecommunications, transportation safety, medical care and financial transactions that may affect national and international security. These contribute to the stability of societies, but they also provide an opportunity to destabilise them, for in modern societies a crisis may not only be sparked by an armed attack but also by a lengthy power cut or a breakdown of banking services.

The importance of critical infrastructure is now relatively well understood. Until the advent of the internet, nothing short of a physical attack or natural disaster could disrupt this infrastructure, but now the widespread use of the internet has added the term "critical information infrastructure" to our vocabularies. As Estonia and some other nations have been unfortunate enough to discover, cyber-attacks have been a reality for some years. And today, a botnet that can direct the capabilities of thousands of computers against any target for sale at a price of some €600 on Russia's cyber-crime black market, it's going to be increasingly easy for cyber-attacks to be launched.

The threat of cyber-attacks using botnets or similar capabilities has become fairly well understood. Measures have been taken by governments and by the international community to enhance the resilience of cyber-space and prevent serious disruption of infrastructures. The need for critical information infrastructure protection (CIIP) is acknowledged worldwide and the creation of cyber-security strategies or specialised cyber-institutions has been widely undertaken. Yet CIIP as it now stands isn't enough to safeguard us for the future. It won't prepare us for the internet of things.

"The increasing ease with which cyber-attacks can be launched means we already have to prepare for more numerous and more complexe cyber attacks in the future."

So what are the new challenges that the internet of things poses for our current way of thinking about CIIP? To start with, critical infrastructure as it's today generally defined is still largely restricted to a select number of important areas, like energy. This also limits the number of systems that are considered necessary to protect, and makes it relatively easier to reinforce their protection. But when the world moves closer to the internet of things, this will complicate CIIP in two major ways.

First, the internet of things increases the amount of systems that will have to be protected exponentially. When repetitive and unnecessary human tasks are given to smart systems, these systems will also become possible targets for cyber-attacks. This is a simple calculation of the number of potentially vulnerable systems that more computerisation would bring. This should not, though, be an argument against moving towards the internet of things, just as potential vulnerability was not an argument when desktop computers replaced typewriters.

Second, and perhaps more important, the internet of things will blur the line between critical information infrastructure and less-critical systems. Even if we protect a power plant from cyber-attack, that would be of no use if the smart systems that regulate an important building come under attack. As these lines begin to blur, we need to re-adjust our cyber-security thinking.

Modern society will also be presented with a growing number of questions on regulation, compliance and liability in connection with securing data and services. All of these issues need a new approach that would increase their resilience. It is important to start thinking about these issues now because experience teaches us that the development of information technology often moves faster than the ability of big organisations like governments and corporations to catch up.

Dealing with the internet of things puts emphasis on inclusiveness and a holistic approach to cyber-security. At the same time, the increasing ease with which cyber-attacks can be launched means we already have to prepare for more numerous and more complex cyber -attacks in the future. It will be necessary to "future-proof" our existing critical information infrastructure as a hedge against still unknown challenges.

This is the gist of Estonia's solution to this whole problem. As well as setting up institutions and structures that deal with today's cyber threats, we know that we need to expand the capability to respond, and also the general understanding of everyone who uses information systems. In other words, everyone. The response capability and flexibility of Estonian cyber security structures is enhanced by the Cyber Defence League (CDL), an organisation of voluntary experts that came together during, and even before, the attacks of 2007. By making this organisation part of the Estonian cyber security network and by encouraging its further development, we have gained important expertise and flexibility. As well as new capabilities, we are aware that it's important to educate people regarding the risks involved in cyberspace, and how to avoid them. This education should be life-long, and should start in pre-school – if a five-year old can use an iPad, he or she should also be taught the basics of "netiquette". The next steps in information systems and online networking will see society becoming more connected every year. Only one third of the world's population was online last year, but it will be close to 100% by 2020. We need to think very hard now about future challenges if we are to make the internet safe for all its users.

Beyond the security vs. privacy debate

Evening debate

19 September 2013, Brussels

Moderator: Giles Merritt; Rapporteur: David Koczij

Speakers

Jens-Henrik Jeppesen

Director European Affairs

Center for Democracy and Technology (CDT)

Jens-Henrik Jeppesen is responsible for managing CDT's engagement with the EU institutions, member states and other European-based international institutions. Prior to his current role with CDT, he worked at Dell, managed Intel's EU Affairs team in Brussels and worked at the American Chamber of Commerce to the EU, on to Am-Cham's committee on digital economy policy.

Jane Holl Lute

former Deputy Secretary of Homeland Security

Department of Homeland Security (DHS)

Jane Lute has over thirty years of military and senior executive experience in the United States government. As the second-highest official for the DHS, she was responsible for operations designed to ensure the cybersecurity of the U.S. territory. Lute is also President and Chief Executive Officer of the Council on CyberSecurity, an independent not-for-profit organization with a global scope committed to the security of an open Internet.

Joe McNamee

Advocacy Coordinator

European Digital Rights

Joe McNamee has worked in the Internet sector almost continually since 1995. In his current role, he works on a wide range of digital civil rights issues such as data protection, data retention, web blocking and intellectual property. He has written articles for Index on Censorship and FiFF Kommunikation, as well as research on the scale and significance of current projects that promote the devolution of online policing powers to Internet intermediaries.

In the wake of the recent revelations concerning the United States' National Security Agency (NSA) scandal, new questions are coming to light about cyber-security, participants heard at the Security and Defence Agenda's (SDA) debate '**Beyond the security vs. privacy debate**'.

"The cyber-security problem is symptomatic of a much wider change in human society," said moderator **Giles Merritt**, Director of the SDA. "Pre-internet national divisions were something that our laws and societies had adapted to quite well. We are now grappling with the big questions of how to deal with the ethics of the internet that transcends these boundaries, with the only certainty being that these questions will become more and more important as the world becomes more and more wired."

"There are 7 billion of us on this planet and there are only five things that claim the active affiliation of a billion or more people – being Chinese, Indian, Catholic, Muslim, and being a Facebook user"

Jane Lute

In reality, noted **Jens-Henrik Jeppesen**, Director of European Affairs at the Centre for Democracy and Technology, there is no debate between security and privacy. "The latest revelations concerning government interference in standards of encryption technology have quite clearly demonstrated that both security and privacy can be undermined by the same actions."

Furthermore, added **Joe McNamee**, Executive Director of European Digital Rights, "our societies are based on democracy, which requires freedom of speech, which in turn requires privacy. If we do not have privacy, we are missing a cornerstone on which our society is based. In other words, when we trade privacy for security, we are in fact seeking to trade security (of our individual rights) for (national) security."

The conversation about cyber-security has been held behind closed doors for far too long, indicated **Jane Lute**, former Deputy Secretary of Homeland Security, Department of Homeland Security. As the role of government in the lives of citizens changes in tandem with the spread of the internet and increases in data storage capacity and cloud computing, space must be made for a more open and inclusive debate.

The impact of global trends on the security vs. privacy debate

As the global penetration of the internet approaches 35%, many countries are witnessing a massive cyber-awakening. This massive growth in internet use – which has reached as high as 70% penetration in North America and Europe – is contributing to the changing role of governments in the lives of citizens, noted Lute.

"There are 7 billion of us on this planet and there are only five things that claim the active affiliation of a billion or more people – being Chinese, Indian, Catholic, Muslim, and being a Facebook user," she stressed. "Of these groups, only Facebook knows its users to any degree; Facebook knows more about its users than national governments typically know about their citizens and our understanding of people online is almost entirely as consumers, not as citizens -- and that must change.

> *"It is excessively difficult to find out exactly what the oversight mechanisms are and how effective they are. This is not a state we can live with as global citizens."*
>
> **Jens-Henrik Jeppesen**

In the digital age, the most powerful actors in cyber-space are high-tech companies. Google, Facebook, and Yahoo, among others, all control more data and connect more individuals than any single government. "Powerful cyber-actors prove that it is the power to connect, not the power to protect, that matters online," she added. "This is meaningful because governments are what they are in part because they have legitimate consolidated control of the power to protect."

For most of the history of the net, the U.S. government that had considerable political and administrative control over the Internet, noted McNamee. The fact that the internet has been able to grow into such an open, inclusive and global platform is owed greatly to the fact that the U.S. government was able to resist the temptation to exploit that control.

Unfortunately, he added, this benevolent stewardship has been lacking in recent years, as

witnessed by the NSA scandal. “We are now faced with breaches of international law and the undermining of everyone’s information security,” he said. “This is not privacy vs. security. This is privacy, transparency, the rule of law, and security against a corrosive, out-of-control security apparatus.”

There are four main trends underlying this paradigm shift and calling into question the status quo of privacy and cyber-security, Jeppesen indicated:

1) Revolutions in storage and data analysis, combined with fears about terrorism and more mundane demands of public-sector organisations. Public authorities argue that they need to collect increasingly massive amounts of data – held mostly by the private sector – in order to extract crucial pieces of information.

2) Transport implications of government demands for data pose unresolved challenges. Any transaction on the internet involving government entities from various countries expressing a legitimate interest in citizens from different geographical areas is likely to create problems for the companies that hold that data.

3) Fibre optic networks, web-based email and other cloud services. Data is increasingly stored and transmitted across borders and through transit countries, contributing to unclear definitions of jurisdiction as concerns data retrieval.

4) International laws and agreements have allowed governments much greater powers to collect data in the name of national security than in ordinary criminal cases.

“What we are seeing,” he concluded, “is a fundamental shift in the surveillance paradigm, away from particularised monitoring to a massive systematic surveillance regime which, within the U.S., violates the U.S. constitution and stretches constitutional frameworks beyond the imagination, making legal oversight impossible.” While U.S. capabilities in this area outstrip those of other countries, this is in fact a global concern, with similar examples to be found in France, Germany, and the United Kingdom.

> *“The issue has become muddied to the point where international and government agencies are breaking laws concerning citizen rights in order to defend those same laws”*
>
> **Joe McNamee**

The NSA scandal has laid bare the wholesale breaches of control of the U.S.’ constitutional safeguards, with global consequences, stressed McNamee. “There is too much tension in the balance between individual security and a national security regime that has effectively declared independence from the people it was created to defend,” he concluded.

As the internet and data technology phenomena grow, there has been a global and near-comprehensive decline in the trust that people have in public-sector organisations, noted Lute. “The global moment of cyber-awakening coincides with a lack of trust in government. This is an issue that must be discussed and resolved sooner rather than later.”

Reconciling citizens and consumers: Trust in the digital age

With the advent of cloud computing and the diminishing importance of national boundaries as regards data storage, cloud providers have become increasingly concerned about losing consumer trust. “Corporations such as Intel flourish if the internet ecosystem flourishes,” Jeppesen said. “At the same time, ensuring that data pertaining to EU citizens remains in EU territory is anathema to the concept of cloud computing,” he added. There is a need to reconcile the benefits for consumers of a free and open internet with the privacy and security of citizens through functioning, legal, and trustworthy surveillance systems.

It is necessary to give up some freedoms for the benefits that surveillance based on massive amounts of data provides, noted Cdr. Kurt Engelen, Vice-President of the Euro-Atlantic Association of Belgium, in an intervention from the audience. “I am not scared about the government using my data,” he said. “When they access private data, they do so to prevent crimes. How can we make it clear to people that it is worth giving up a part of their privacy?”

To address that question and provide perspective, one must compare and contrast the online and offline worlds, Jeppesen said, likening the massive collection of data by government agencies to the notion that every letter one receives or sends could be registered at the post office. “It is likely that there is nothing to worry about, but the NSA

scandal suggests otherwise," he stressed. "You have to put a lot of trust in the people who collect and store your data."

A fair representation of the argument for data surveillance is that governments are searching for the terrorist needle in the citizen haystack. While this argument may be valid, the critical element of the issue is what happens to all the other data that is collected in the process. "If the national security officials in charge of this data come across another piece of data that looks suspicious, they may launch an inquest into non-terror-related activities," he concluded.

"The existence of a database is a greater security threat than having no database at all," stressed McNamee. "Yes, one might find fifteen strands of straw that look like needles but are not, and fifteen lives can be ruined." As an argument in support of this, he cited examples of police and tax authorities in Ireland abusing database privileges to stalk and harass innocent citizens.

Underlying the trust issue are the divergent social views on questions of privacy and the relationship between citizen and state, Lute indicated. For example, EU countries issue national identity cards, whereas in the U.S. this would be unthinkable, and companies in the EU are required by law to hand over data to a greater degree than their counterparts in North America.

"This is no time for silence. People on the internet are almost entirely consumers and not citizens. The time is coming for us to change that."

Jane Lute

"We have to determine what our comfort levels are as regards government intrusion in our lives as citizens," she concluded. "It is a false choice between privacy and security. We must reconcile the practical aspects of the discussion."

Moving forward in the security vs. privacy discussion

The first step towards finding workable global solutions to these questions is to reconcile fundamentally different views of privacy between governments, citizens, and both public- and private-sector organisations. Furthermore, noted Lute, citizens must seek to define what expectations they hold for governments in cyberspace, and how to narrate the value proposition of governments in their own lives.

"We as the public need to become better informed," she concluded. "Normally governments are charged with security – managing police forces and the military. While this is true for most 'spaces', it has not thus far been true for cyberspace. We must begin by asking ourselves how do we assign responsibility for our cyber-security?"

In the case of the NSA, there is supposed to be oversight but, Jeppesen stressed, but by their own admission, these overseeing bodies have not been able to perform their function. "There is a tremendous amount of work that needs to be done in terms of reining in these surveillance programs," he said. "It is excessively difficult to find out exactly what the oversight mechanisms are and how effective they are. This is not a state we can live with as global citizens."

He urges an international debate on how to handle the issue, beginning with the EU and the U.S., as the foremost proponents of the rule of law and global human rights. "The best way forward can be found in the context of international human rights law," he said. "International human rights treaties recognise the right to privacy and they also say that this right is not absolute."

The European Court of Human Rights says that public authorities can interfere with the right to privacy for national security purposes in accordance with the law, when necessary. "What this means is not clear at the moment," he concluded. "We need more transparency in order to have an informed debate."

"The truth is that the NSA has admitted that, in the twelve months prior to May 2012, there were 2.776 breaches of data as a result of their activities," McNamee underlined. "I think the EU and the US are well-placed to take a lead in solving the cyber-security problem. However, the current practices have done too much damage to their credibility worldwide."

"The issue has become muddied to the point where international and government agencies are breaking laws concerning citizen rights in order to defend those same laws," he concluded. "What are needed are necessity, proportionality, and a fresh look at digital privacy rights, based on international human rights principles."

"What is doing severe damage to the openness of the internet are not the revelations," concluded Lute. "What is doing damage to you and me every day are the criminals who are online. This is no time for silence. People on the internet are almost entirely consumers and not citizens. The time is coming for us to change that."

Wanted: Cyber-security professional

Evening debate

14 November 2013, Brussels

Moderator: Giles Merritt, Rapporteur: Christopher Dalby

Speakers

Amelia Andersdotter
Member, Industry, Research and Energy Committee (ITRE)
European Parliament

Internet freedom, a future-minded IT-policy, freer access to knowledge and culture, increased investments in science and research and a more intelligent industrial policy are some of the issues Andersdotter is passionate about. She is a member of the committee for industry and research (ITRE) of the European Parliament and of the Swedish Pirate party. She has been named one of the worlds ten most important internet activists for 2012.

Brigadier General Bruce T. Crawford
Director for Cyber-security
U.S. European Commmand (USEUCOM)

Brig. Gen. Crawford is responsible for directing the employment and activities of assigned, attached and support cyber forces to ensure the integ<rated planning, synchronization, monitoring and assessment of joint cyber operations within USEUCOM's area of responsibility.

Patryk Pawlak
Senior Analyst
European Union Institute for Security Studies (EUISS)

Pawlak deals with internal security policies of the EU, in particular border protection, counterterrorism and cybersecurity. Prior to joining the EUISS, he was a visiting scholar at numerous research institutions, including the Center for Transatlantic Relations (Washington, DC), the Center for Peace and Security Studies at Georgetown University (Washington, DC) and the Centre for European Policy Studies (Brussels).

Jamie Shea
Deputy Assistant Secretary General for Emerging Security Challenges
North Atlantic Treaty Organization

Shea held several senior positions at the North Atlantic Treaty Organization prior to his current one, including Director of Policy Planning in the Private Office of the Secretary General. He also holds a number of academic position, most notably with the Collège d'Europe in Bruges.

The SDA's 2012 Security Jam, the massive online debate which brought together some 4,000 participants over a four day period, identified the hiring of cyber-security professionals as a top priority. The SDA picked up this theme and brought together over one hundred senior representatives from NATO, EU institutions, national governments, industry, NGOs, academia and the media to discuss solutions

SDA Director **Giles Merritt** highlighted the gravity of the problem by citing that "more than 20% of the US Department of Homeland Security's cyber jobs are unfilled". In light of this obvious deficit he questioned whether pay was a contributing issue.

Brig. Gen. Bruce T. Crawford, EUCOM Director for Cyber-Security stated that the cyber challenge "is unlike any other that we face today, and so we have to apply some new thinking to this challenge."

Firstly he championed that manning, training, equipment, and organisation for the cyber challenge is an investment, and must be seen as such by governments and organisations. Secondly, in recruiting for the cyber profession, he emphasised that the general public needs to be made aware of and educated about the concept of cyber, and that some demystifying needs to be done.

Crawford insisted that raising interest in cyber needs to occur at a younger age, and that steps should be taken to generate the intellectual curiosity necessary in educational institutions. He explained that the problem isn't "about pay, but more about generating

> *"A lot of youngsters out there are digital natives – they know of nothing but the digital world – so this has more to do with them being interested in general, not just about their pocket book."*
>
> **Brig. Gen. Bruce T. Crawford**

interest – a lot of youngsters out there are digital natives, they know of nothing but the digital world, so this has more to do with them being interested in general, not just in their pocket book." Demystifying the cyber field and showing people what they are really doing and what the value added is in their participation can, he believes, go a long way to creating an inherent interest in cyber professions.

Amelia Andersdotter, Swedish Member of the European Parliament, added that part of the "fundamental challenges in the field of information and communications policy is that the word cyber is too cool." She rhetorically asked if Edward Snowden and Bradley Manning's revelations were not their attempt to demystify the cyber field. However, in doing so their actions caused a highly traumatic debate in society about cyber, which additionally has caused many problems for industry actors trying to create future markets for consumers and citizens.

Andersdotter reasoned that part of the problem is that "our law enforcement agencies and military complexes are now surrounded by legislation that encourages them to attack networks, hack and spy. In turn it incentivises the creation of hacking tools that exploit and sell vulnerabilities and make surveillance tools." The on-going policy debate has not yielded results, with Member States and institutions fighting to keep the intelligence privileges they were given post 9/11. This "extremely hostile environment" is the cause of unfilled jobs rather than a lack of interest in the information communication technologies sector.

> *"The on-going policy debate has not yielded results, with Member States and institutions fighting to keep the intelligence privileges they were given post 9/11. This extremely hostile environment is the cause of unfilled jobs."*
>
> **Amelia Andersdotter**

Merritt asked if what keeps political leaders awake at night isn't the possibility that "critical infrastructures could suddenly grind to a halt because [there aren't] enough people defending the ICT systems that make these things work?" rather than surveillance and intelligence gathering?

"There is no accountability for software vendors in the field of critical infrastructure "replied Andersdotter, unlike in the airline and shipping industries. This makes no sense, as surely if a product has vulnerabilities in it then its creators should be held liable.

Patryk Pawlak, a senior analyst at the European Union Institute for Security Studies, admitted that in his view “there is actually no such thing as one cyber professional, and this is part of the problem.” Cyber is often presented as something that can only be done by either programmers or engineers. The reality is that there are many professions which contribute to a more secure cyberspace . He suggested that the best way to demystify the cyber profession is to steer away from defining it as the profession too narrowly but rather focus on the different avenues of employment. “When talking about cyber professionals we are talking about diplomats, law enforcement agents, the development community, engineers, and teachers […] there is no one answer as it is a horizontal responsibility,” he stated. Some professions are more advanced in clarifying their contributions to cyber while others are still struggling to find their place.

Pawlak indicated that some of the solutions already on the table already contribute – directly or indirectly - to generating cyber workforce and qualifications. For instance the Network and Information Security (NIS) Directive proposes a voluntary frameworks such as the NIS Driving License or imposes obligations on Member States, de facto forcing them to generate the necessary labour force. This would have a bonus effect of raising education standards and awareness about the cyber profession. Those same skills and capabilities are generated through exercises such as those regularly carried out by ENISA or individual member states.

> *“There is actually no such thing as a cyber professional, and this is part of the problem. […] We are talking about diplomats, law enforcement agents, the development community, engineers, and teachers .”*
>
> **Patryk Pawlak**

Pawlak also had a few recommendations of his own; developing a universally understood ethos for cyber professionals – similar to the civil servants status - was identified as a fundamental need. “When you think about it […] these are often people with access to information about millions of citizens, and they can do many things with it. Recognising their service and building up their reputation may constitute an important incentive where financial gratification is limited” Pawlak reasoned.

Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges at NATO, insisted that cyber is the area where you cannot handle the threat from within

your own community in the same sense that you can handle missile threats or conventional threats from within your own community. He believes that concerning "the cyber domain it is not just [a question of] do I have the right people, and do I have enough of them - to which the answer is no I think for virtually everybody - but do I have the right network outside of my organisation, so that I am getting up-to-date information about threats, and the relevant tip offs?"

He went on to explain that NATO benefits, like many other organizations, from the white hats or cyber amateurs etc, who just call up and report possible vulnerabilities that they think NATO might not have previously been aware of. He emphasised that the cyber business today is really about who you know, who is willing to help you, how good your contacts are and how willing your are to keep them up. He also noted that "we occasionally get tip offs from very unlikely sources. Though often these are the same people who can tip the other way."

> "We occasionally get tip offs from very unlikely sources. Though often these are the same people who can tip the other way."
>
> **Jamie Shea**

It is also about the quality of partnerships with industry, the ability to reach out across industry and governments for malware sharing platforms, confidential data exchange systems etc. Operators need to be able to go to the intelligence community and flag potential threats and vice-versa.

An important problem in evaluating cyber threats is the complete absence of a reliable base line metric. Without it there is no real way to evaluate a threat, the actual damage inflicted**,** or how many specialists are needed to mitigate it. Defence should not solely rely on how many people are needed but rather ensuring the right mix of skills and a general cyber-defence culture throughout the organisation.

Anne-Sophie Bernard, from the European Commission's DG Connect, spoke about the NIS driving licence, a certification programme to recognise cyber-security skills, meant to help facilitate the movement of these skills across Europe, the cyber security championship, and the European cyber-security month. Andersdotter added that working with computers is to be made 'cool' at school, targeting girls in particular.

Pawlak added that cyber is too often discussed only from the military and defence perspective. "The discussion turns immediately to discussion about cyber-conflict, cyber-war, the defence industry and so on [...] rather than talking about the loss of intellectual property due to cyber-espionage, companies going out of business because their commercial secrets are being stolen ."

A representative of the European External Action Service asked if the outsourcing of IT needs, as done by U.S. agencies, could be the answer to the needs of EU/NATO Member

States? The panellists generally agreed that outsourcing was not the answer but that there should be internal cyber-capabilities across the public-private divide.

Merritt summarised that "we are very unsure what the problem is exactly, and until something goes very wrong we won't start to crystallise our thinking, which then might be around yesterday's problem rather than tomorrow's."

List of participants 2013

Emil Akander
Project Manager, Swedish Trade and Invest Council

Farnaz Alimehri
Student, Vesalius College

Charlotte Allen
Official, European External Action Service (EEAS)

Ana Arana Antelo
Head of Unit, Research Infrastructure, European Commission, Directorate General for Research and Innovation

Andrius Avizius
Director, Committee on the Civil Dimension of Security, NATO Parliamentary Assembly

Eda Aygen
Communication Manager, European Organisation for Security (EOS),

Joaquín Azcárraga Gonzalo
Assistant to Antonio López-Istúriz MEP, European Parliament

Oana Badan
Assistant, Council of the European Union, General Secretariat

Mohamed-Raja'l Barakat
Independent Economic Expert

Viorel Barbu
ICT Security Expert, Council of the European Union

Oxana Bartels
Policy Officer, European Commission, Directorate General for Fisheries & Maritime Affairs

Dragos Basmaluta
Chief Executive Officer, Mira Telecom

Alexandra Beaulieu
Researcher, Hobart and William Smith Colleges

Joanna Beczala
Administrator, International Relations Officer, European Commission, Directorate General for Home Affairs

Delphine Beyen
Student, Vesalius College

Dominika Bezakova
Legal Assistant, European Commission, Directorate General for Health and Consumers

John Bird
Department of Homeland Security Attaché to the EU & NATO, Mission of the United States of America to the EU

Henrik Bliddal
Director, Science and Technology Committee, NATO Parliamentary Assembly

Giorgio Bombassei
Independent Researcher and Writer

Elena Bossi
Project Assistant, Friends of Europe

Kris Boulez
Senior Manager, PWC

Jake Braun
Executive Vice President, Resolute Consulting

Margaret Brusasco-Mackenzie
Senior Advisor, Institute for Environmental Security

Martin Buggy
Assistant to James Elles MEP, European Parliament

Olivier Bulto
Senior Analyst, K City

Richard Caine
Policy Officer, European Commission, Directorate General for Home Affairs

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

Joannie Caron
Assistant, Political section, Mission of Canada to the EU

List of participants 2013

Mario N. Castellon
Research Assistant, University of Leiden, Centre for Terrorism and Counterterrorism

Lt.Fabio Casula
Human Factor Analysis, Psy. Operations, Ministry of Defence, Belgium

Pavel Chervonobab
First Secretary, Mission of the Russian Federation to NATO

Jessica Chetelat
Researcher, Furman University

Jeffrey Cima
Executive Officer, United States Mission to NATO

Colin Cogitore
Intern, Interpeace

Paul Cohen
Project Assistant, Security & Defence Agenda (SDA)

Maruša Conič
Assistant, Ludwig von Mises Institute Europe

Robert Cox
Trustee, Friends of Europe

Brig. Gen.Bruce T. Crawford
Director for cyber-security, U.S. European Command (USEUCOM)

Adrian Croft
European Defence Editor, Thomson Reuters

Atu Darko
Director EU Affairs, Flying Bridges

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

Antonio De Palmas
President EU & NATO Relations, Boeing

Amb. Jean De Ruyt
Senior European Policy Adviser, Covington & Burling

Elizabeth Dengal
Researcher, Hobart and William Smith Colleges

Eva Diaz Perez
Vice-President Head of Sales EU & NATO Affairs, EADS Cassidian

Utku Dogan
Assistant, Turkish Industry and Business Association (TÜSIAD)

Rafal Domisiewicz
Policy Officer, European External Action Service (EEAS), Directorate for Americas

Gaël du Bouëtiez
External Speaker, European Commission

Amb. Sorin Dumitru Ducaru
Assistant Secretary General, North Atlantic Treaty Organization (NATO), Emerging Security Challenges Division (ESCD)

Eliot Edwards
Senior Associate, Interel European Affairs

Maria Elena Efthymiou
Administrator, Committee on Security and Defence, European Parliament

Mohamed El Khyaru
Military Attaché, Embassy of Morocco to Belgium

Elina Eloranta
Researcher, University of Tampere

Kurt Engelen
Vice-President, Euro-Atlantic Association of Belgium

Mikhail Evteev
Third Secretary, Mission of the Russian Federation to NATO

Afonso Ferreira
Policy Officer, European Commission, Directorate General for Communications Networks, Content and Technology

David Fouquet
Senior Associate, European Institute for Asian Studies (EIAS)

List of participants 2013

Evangelos Freskos
CIS Security Contractor, North Atlantic Treaty Organization (NATO), NATO Communications and Information Agency (NCIA)

Maximilian Freudenthaler
Seminar Assistant, Friedrich-Ebert-Stiftung (FES) EU Office

Anna-Karin Friis
Freelance Journalist

Daniel Furby
Senior Account Executive, Fipra International

Faustine Gauthier
Legal Assistant, European Commission

Myles Geiran
Deputy Head of Mission, Mission of Ireland to NATO

Dan Gherasim
InfoSec Manager, Council of the European Union

Andrea Ghianda
Outreach & Events Manager, Security & Defence Agenda (SDA)

Laurent Giquello
Programme Manager, European External Action Service (EEAS), Crisis Management and Planning Directorate (CMPD)

Adam Gono
Assistant to the Secretary General, European Liberal Youth (LYMEC)

Virginie Goupy
Journalist, Europolitics

Brigid Grauman
Independent journalist

David Grivet
Research Analyst, Mission of South Korea to the EU

Wilfried Grommen
Director & CTO, Hewlett Packard

Col. Richard Gruber
Counsellor, Military Affairs, Mission of Austria to NATO

Victorine Hage
Assistant, Atlantic Treaty Association (ATA)

Ben Hale
First Secretary, Security, Permanent Representation of the United Kingdom to the EU

Monica Hargis
Senior Partner, Marketosis

Col. (Ret.) Marco Hekkens
Independent Maritime Security Adviser

Maria Hidalgo Bautista
Assistant, European Parliament, Committee on Foreign Affairs

Tuija Hirvonen
Consultant, Cognizant

Jeroen Hoes
Attaché, Ministry of Foreign Affairs, Belgium

Cătălin Doru Hrișcă
Desk Officer, Romanian Cultural Institute

Justin Hustwitt
Counsellor, Permanent Representation of the United Kingdom to the EU

Alina Iatan
Programme Manager, Cyber Security, European Committee for Electrotechnical Standardization (CENELEC)

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

Jens-Henrik Jeppesen
Representative and Director for European Affairs, Center for Democracy and Technology

Lucie Kadlecova
Assistant, European Commission, Cabinet of EU Commissioner Stefan Füle

List of participants 2013

Barbara Kaudel-Jensen
Deputy Head of Mission, Mission of Austria to NATO

Arianna S. Khatchadourian
Independant researcher

Anna Kilan-Lipka
Second Secretary, Political Division, Permanent Representation of Poland to the EU

Péter Király
Assistant, Public Affairs, Permanent Representation of Hungary to the EU

Cem Kocer
Researcher, Centre d'etudes des Relations Internationales et Stratégiques (CERIS)

Axel Koehler
Cyber Security Officer, Ministry of Internal Affairs and Sports of Lower Saxony

Marion Kokel
Assistant, European Parliament

Dobrin Komitov
Seconded National Expert, European External Action Service (EEAS)

Daria Kovarikova
Political Officer, Embassy of the United States of America to Belgium

Hannes Krause
Assistant Defence Counsellor, Delegation of Estonia to NATO

Yury Kukharenko
First Secretary, Mission of the Russian Federation to NATO

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

Kajsa Larsson
Swedish Pirate Party

Alexis Letulier
IT Director, European Union Satellite Centre (EUSC)

Vesna Ljungquist
Administrative Coordination Assistant, Children's rights, European Commission, Directorate General for Home Affairs

Annieke Logtenberg
Assistant, Security Policy and Research, European Commission, Directorate General for Enterprise and Industry

Clotilde Lombardi Satriani
Vice President, Agenzia d'Informazione Europea

Jan Louzek
Assistant to MEP Amelia Andersdotter, European Parliament

David Luengo Riesco
Head of Brussels Office, Indra

Amb. Douglas Lute
Permanent Representative, United States Mission to NATO

Jane Holl Lute
President, Council on CyberSecurity

Shaoxuan Ma
First Secretary, Mission of the People's Republic of China to the EU

Consiglia Maciariello
Assistant, European Parliament

Friedl Maertens
European Union Business Development Executive, IBM Belgium

Natalia Marczewska
Consultant, North Atlantic Treaty Organization (NATO), Political Affairs and Security Policy Division (PASP)

Pauline Massart
Deputy Director, Security & Defence Agenda (SDA)

Burak Matsar
Second secretary, Embassy of Turkey to Belgium

Levi Maxey
Student, Vrije Universiteit Brussel (VUB)

List of participants 2013

Joe McNamee
Executive Director, European Digital Rights (EDRI)

Gabriel Moldoveanu
Counsellor, Delegation of Romania to NATO

Ignacio Montiel-Sanchez
R&T Technology Manager, European Defence Agency (EDA)

Victor Moscovoy
Officer, Cyber Defence Section, North Atlantic Treaty Organization (NATO), Emerging Security Challenges Division (ESCD)

Valérie Moutal
Business Continuity Coordinator, European Commission, Directorate General Human Resources and Security

Sinan Mueller-Karpe
Assistant, Representation of the State of Hessen to the EU

Jörg Müller
Head of Unit for use and traffic matters, Ministry of Internal Affairs and Sports of Lower Saxony

Molly Nadolski
Policy Analyst, Global Governance Institute

Eva Nagyfejeo
Assistant, European Parliament, Committee on Security and Defence

Christopher Newman
Editorial Assistant, Europe's World

Nikolaj Nielsen
Journalist, EUobserver.com

Mihai Costin Nitoi
Counsellor, Cyber Security, EU Internal Security, Permanent Representation of Romania to the EU

Roy Nitze
Second Secretary, Permanent Representation of Germany to the EU

Staša Novak
Assistant Defence Advisor, Delegation of Slovenia to NATO

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

Andrey Ognev
First Secretary, Mission of the Russian Federation to NATO

Kristiina Ojuland
Member, Committee on Foreign Affairs, European Parliament

Volodymyr Orativskyi
Counsellor, Mission of Ukraine to NATO

Laszlo Orosz
Second Secretary, Permanent Representation of Hungary to the EU

Pavel Palencar
Diplomat, Permanent Representation of the Slovak Republic to the EU

Areva Paronjana
Project Assistant, Security & Defence Agenda (SDA)

Patryk Pawlak
Senior Analyst, European Union Institute for Security Studies (EUISS)

Dragos Peica
Head of Section "Methodology, Quality Assurance & Risk Management", European Commission, Directorate General for Research and Innovation

Amy Pipher
Student, Vesalius College

Detlef Puhl
Senior Advisor, Strategic Communications, North Atlantic Treaty Organization (NATO), Emerging Security Challenges Division (ESCD)

Col.Yi Qiu
Counsellor, Mission of the People's Republic of China to the EU

Diane Remaley
Second Secretary, Embassy of the United States of America to Belgium

List of participants 2013

Peter Rezo
First Secretary, Embassy of Slovak Republic to Belgium

Eberhard Rhein
Honorary Trustee, Friends of Europe

William Roelants de Stappers
Deputy Permanent Representative, Delegation of Belgium to NATO

Wolfgang Roering
Project Officer, Cyber Defence, European Defence Agency (EDA)

Jeffrey Rogers
Business Development Executive, Raytheon Systems

Christy Romer
Assistant, Political Intelligence

Paula Roth
Swedish Pirate Party

Anna Rozenich
Independant Researcher and writer

Lailuma Sadid
Freelance Journalist, 8morning

Elena Safronova
Second Secretary, Mission of the Russian Federation to the EU

Jonathan Sage
Government Programmes Executive, IBM UK

Brig. Gen. Giuseppe Santomartino
Director CIS, European External Action Service (EEAS), European Union Military Staff (EUMS)

Donald Scargill
Director, Information2Intelligence

Martha Scheja
Researcher, International Relations, University of Kent, Brussels School of International Studies (BSIS)

Charles Schmidt
Student, Vesalius College

Teri Schultz
Freelance Reporter, National Public Radio (NPR)

Elsa Serna
Independent Researcher

Angela Seychell
Researcher, Vesalius College

Jamie Shea
Deputy Assistant Secretary General, North Atlantic Treaty Organization (NATO), Emerging Security Challenges Division (ESCD)

Catherine Sheahan
Junior Analyst, European Union Institute for Security Studies (EUISS)

Col. James Shigekane
Air Attaché, Embassy of the United States of America to Belgium

Michael Sieber
Deputy Director, R&T, European Defence Agency (EDA)

Aleksander Siemaszko
Project Assistant, Security & Defence Agenda (SDA)

Aldo Siragusa
Former Head of Division, Council of the European Union

Capt. Bart Smedts
Research Fellow, Royal Higher Institute for Defence, Belgium

Olivier Snoy
Researcher, Computer Science and Networks, Enseignement de Promotion et de Formation Continue

Leonid Sokolnikov
Journalist, Academy Europe Media

René Steiner
Administrator, European Commission, Directorate General Human Resources and Security

List of participants 2013

Sebastian Stodulka
Assistant, European Commission

Anne-Claire Streck
Project Coordinator, Bouygues EU Affairs

Colin Sweet
PhD Researcher, University of Glasgow

Nagayo Taniguchi
Journalist, SEKAI

Col. Vasily Tarakanov
Assistant Defence Attaché, Mission of the Russian Federation to the EU

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

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

John Tod
Former Director of the British Council, France

Avgustina Tzvetkova
Senior Consultant, Defence and Security Programme, and former Bulgarian Deputy Defence Minister, Transparency International

Leendert van Bochoven
NATO and European Defence Leader, IBM Europe

Anna van Densky
Correspondent, EU Reporter

Ulrich van Essen
Head of Unit, Protection of EUSI, Council of the European Union, General Secretariat

Lt. Gen. Ton van Osch
Former Director General of EUMS

Willem van Sluijs
Counsellor for Interior Affairs, Permanent Representation of the Netherlands to the EU

Wout Van Wijk
EU Public Affairs Manager, Huawei Technologies

Nicolas Vandaele
Commissioner-Auditor, Standing Intelligence Agencies Review Committee, Belgium

Bart Vande Ghinste
Enterprise Architect - Evangelism Manager, Microsoft

Ziggy Vandebriel
Analyst, Global Governance Institute

Cecilia Verkleij
Head of Sector, European Commission, Directorate General for Home Affairs

Luc Véron
Advisor, European External Action Service (EEAS)

Vyta Vinciene
Director, E-Projects Centre (EPC) for Security and Defence

Konstantin V. Vorontsov
Second Secretary, Mission of the Russian Federation to NATO

Kostyantyn Voytovsky
Counsellor, Mission of Ukraine to NATO

Diana Wanjiku
Student, Vesalius College

Lt. Col.Krzysztof Wawruch
Military Representative, Delegation of Poland to NATO

Christiaan Weiland
Senior Policy Advisor, Fleishman-Hillard

Wim Wensink
Principal Manager, PWC

Ian West
Director, North Atlantic Treaty Organization (NATO), Communications and Information (NCI) Agency

Wendy Wiel
Consultant assistant, Political Intelligence

List of participants 2013

Lorraine Wilkinson
Senior Account Manager, Fleishman-Hillard

Katerina Wright
Senior Analyst, The Avascent Group

Yorck Wurms
Analyst, Home Affairs, Representation of the Region of Lower Saxony to the EU

Annemarie Zielstra
Local Counsellor, VVD Hilversum

Sophie Zimmer
Assistant, European Parliament, Committee on Budgets

Trina Zwicker
Cyber Public-Private Partnership, U.S. European Command (USEUCOM)

The SDA would like to thank those partners

who have supported the cyber initiative from its inception:

Europe's World | Finmeccanica| Huawei | IBM | McAfee

Microsoft | NATO | Raytheon | TNO

In 2014

Below is an outline of some of the activities scheduled. Please check our website regularly for updates.

20 January

Cross-border crime and corruption in Europe:
what next after the Stockholm Programme?

Roundtable, Berlin - Organised in cooperation with *Friends of Europe* and the European Commission's Directorate General for Home Affairs (DG HOME)

February

Cyber-security technologies –What does tomorrow have in store

Evening debate

April

Facing up to cyber-risk

Evening debate

5 June

The next security era

International conference

October

Insurance and liability in the cyber-age

Evening debate

Turkey as a regional, political and industrial power

Roundtable, 2-6 June

November

China's developing security role,

International conference, 5 june

Personal data protection: Necessity, proportionality and digital privacy rights

Evening debate

SDA
SECURITY & DEFENCE AGENDA

The Security & Defence Agenda (SDA)

would like to thank its members and partners for their support

NATO OTAN | European Commission | Konrad Adenauer Stiftung | IBM | EUROPEAN DEFENCE AGENCY

FINMECCANICA | EADS | pwc | BOEING | Raytheon

THALES | indra | DCNS | Avio | CISCO

United Technologies | ASD | NORTHROP GRUMMAN | BAE SYSTEMS

Mira Telecom Integrated Telecommunications & Security | Honeywell | hp | MBDA MISSILE SYSTEMS | AVASCENT

eutelsat COMMUNICATIONS | SAIC | CEIS | STRATEGY ANALYTICS ...insights for success

CEEP Central Europe Energy Partners | INTERPOL | ATLANTIC COUNCIL | BRITISH COUNCIL | sipri

friends of europe les amis de l'europe | BertelsmannStiftung | ISN ETH Zurich | THE CHICAGO COUNCIL ON GLOBAL AFFAIRS | Europe's World

CSIS CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | RUSI | GCSP | DCAF | The Hague Centre for Strategic Studies | EGMONT

CIDOB Barcelona Centre for International Affairs | FONDATION pour la RECHERCHE STRATÉGIQUE | Hanns Seidel Stiftung | DiploNews | FOI | isis europe

CARNEGIE EUROPE CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE WASHINGTON DC • MOSCOW • BEIJING • BEIRUT • BRUSSELS | 50 SWP 1962–2012 | CHATHAM HOUSE Independent thinking on international affairs | GALLUP | SECURITY EUROPE

The SDA gratefully acknowledges the generous support of the following governments:

Belgium | Czech Republic | Finland | France | Georgia| Italy | Netherlands
Poland | Qatar | Romania | Russia | Sweden | Turkey | United States | United Kingdom

For further information on SDA membership, contact us at:

Tel: +32 (0)2 300 29 91 | E-mail: info@securitydefenceagenda.org

SECURITY & DEFENCE AGENDA (SDA)

4, rue de la Science 1000 Brussels, Belgium
Tel: +32 (0)2 300.29.91 Fax: +32 (0)2 300.29.90 E-mail: info@securitydefenceagenda.org

www.securitydefenceagenda.org
www.facebook.com/s.d.agenda

@secdefagenda