SECURITY & DEFENCE AGENDA

Cyber-protection of critical infrastructure

Report

October 2012

In partnership with:

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

A *Security & Defence Agenda* Report
Rapporteur: Seán Smith
Photos: François de Ribaucourt
Publisher: Geert Cami
Date of publication: October 2012

SECURITY & DEFENCE AGENDA
Bibliothèque Solvay, Parc Léopold,
137 rue Belliard, B-1040, Brussels, Belgium
T: +32 (0)2 737 91 48
F: +32 (0)2 736 32 16
E: info@securitydefenceagenda.org
W: www.securitydefenceagenda.org
Follow us on Twitter @secdefagenda

Programme

This policymakers' dinner marked the end of the first year of the SDA's cyber-security initiative, which concentrated on defining cyber-security and the most prominent threats, as well as the interactions between the private and public sectors. Most cyber-attacks have so far had criminal and financial motives, but for governments the nightmare scenario remains an attack on critical infrastructure. Is a radical approach like cutting such networks off the 'public' internet the best solution and could developments like smart grids aggravate this threat? What innovations could make critical infrastructure systems more resilient? Have insurers been party to international governance discussions, and what can software producers do to improve cyber defences? Is the idea of an EU-wide rapid reaction force for cyber-attacks feasible, or even desirable?

Introductory remarks by:

Helena Lindberg, Director General, Swedish Civil Contingencies Agency
Pauline Neville-Jones, Special Representative to Business on Cyber Security, Cabinet Office, United Kingdom
Annemarie Zielstra, Director, Centre for Protection of the National Infrastructure, The Netherlands

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

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

Speakers & moderator

Helena Lindberg
Director General
Swedish Civil Contingencies Agency

Helena Lindberg has been the Director General of the Swedish Civil Contingencies Agency since its launch in January 2009. She was previously the Director General of the Swedish Rescue Services Agency (SRSA) and the Swedish Emergency Management Agency (SEMA). From 2003 – 2008 she served as permanent under-secretary at the Ministry of Defence and between 2001- 2003, was chief legal adviser at the Swedish Government Secretariat for Intelligence Co-ordination.

She has also worked as a chief legal adviser at the Swedish Security Service. In addition, Lindberg has served as the deputy director at the Ministry of Justice and worked as an Associated Judge of Appeal at the Svea Court of Appeal in Stockholm.

She has a Master of Laws degree from Stockholm University.

Baroness Pauline Neville-Jones
Special Representative to Business on Cyber Security
Cabinet Office, United Kingdom

Baroness Neville-Jones has been the U.K. Cabinet Office's Special Representative to Business on Cyber Security since May 2011. She is also patron to Cyber Security Challenge since its inception in 2010.

Neville-Jones is a former BBC Governor and Chairman of the Joint Intelligence Committee (JIC). In May 2010, she was appointed Minister of State for Security and Counter Terrorism at the Home Office with a permanent position on the newly created National Security Council.

Neville-Jones was a career member of HM Diplomatic Service from 1963 to 1996, during which time she served in British missions in Rhodesia, Singapore, Washington, DC and Bonn. Between 1977 and 1982 she was seconded to the European Commission where she worked as Deputy and then Head of Cabinet to Commissioner Christopher Tugendhat.

From 1991 to 1994 she was Head of the Defence and Overseas Secretariat in the Cabinet Office and Deputy Secretary to the Cabinet. During 1993 and 1994 she was Chairman of the Joint Intelligence Committee. From 1994, until her retirement, she was Political Director in the Foreign and Commonwealth Office, in which capacity she led the British delegation to the Dayton negotiations on the Bosnia peace settlement. As chairman of QinetiQ Group Plc., Neville-Jones took the company to flotation as a FTSE 250 company in 2006.

Speakers & moderator

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

Annemarie Zielstra is the Director of the Dutch Centre for Protection of the National Infrastructure (CPNI.NL). She has spent the last 11 years as programme manager for different ICT programmes in the public sector.

Since 2006, Zielstra has been working within the Dutch Government to help protect critical national infrastructure. As a programme manager NICC in 2006-2010, and later as director of CPNI.NL, Zielstra was responsible for setting up a national infrastructure within the Cybercrime Information Exchange. She established a model for information sharing between public and private organisations.

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

Giles Merritt
Director
Security & Defence Agenda

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

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

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

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

Cyber-protection of critical infrastructure

The SDA welcomed the Rt. Hon. Pauline Neville-Jones and other top cyber-security experts to a dinner debate as part of the SDA's cyber-security initiative.

SDA Director Giles Merritt began by asking: "How do you distinguish between cyber-security and cyber-crime? How do you ensure that all the players are communicating with each other? What sort of rules should we be going for?"

Helena Lindberg, Director General of the Swedish Civil Contingencies Agency, set the scene for the evening by sketching out the bleak scenario of a serious critical infrastructure failure.

"What if the really big one strikes? How many of our contingency plans would hold for instance in the situation of a long-term electricity break-down? How resilient would our societies be after perhaps a month of disruption? Do we have any idea of the cascading effects or the interdependencies of such a frightening scenario? I don't think we really do."

She reminded everyone that this has actually happened before, invoking the Carrington event of 1859, when an extremely powerful solar storm brought down telegraph systems all over Europe and North America for several days. With our hyper-reliance on electronics and telecommunications, how would today's global society deal with such a collapse? "The cyber consequences of an extreme space weather event in the 21st century are likely to be catastrophic."

In her opening remarks, Neville Jones drew a parallel between the setting for the dinner and her government's strategy for addressing the issue of cyber-security, in what was to become one of the strongest themes of the debate:

"I think this boardroom-style setting is rather appropriate because my focus has been on relationship between government and private sector in the sphere of cyber-security. Our main priority is to get cyber-security into the boardroom."

"Our main priority is to get cyber-security into the boardroom…a large number of senior managements don't regard this as their responsibility"

Pauline Neville-Jones

She explained how she has sought to bring about a change of mentality so that, rather than people and firms viewing cyber-security as a burden, they see it as an enabler of their business. She emphasised that people need to realise this is something of vital importance to them which will actually save them expense and embarrassment. Otherwise, "reputationally, as a company, you can be ruined."

"There is no substitute for prevention because once something has happened, you are in dead trouble."

According to Neville-Jones, the central question is, "Are companies taking this seriously?" To ascertain this, CEOs and business leaders should ask themselves: "Do I know what's going on in my business? Do I know what the system looks like when it functions normally, so that I know what abnormal looks like, so that I can actually detect and identify an anomaly?"

Her current assessment is that, "an awful lot [of business leaders] cannot do this", principally because, "a large number of senior managements don't regard this as their responsibility".

Annemarie Zielstra, Director of the Dutch Centre for Protection of the National Infrastructure, built upon this point. She called for a greater culture of information-sharing within organisations and lamented the prevailing orthodoxy: "There is no culture yet because technical people are hired to keep the problems out of the boardroom."

"There is no culture [of information-sharing] yet because technical people are hired to keep the problems out of the boardroom…cyber-resilience is not a technical issue, but a shared responsibility within the organisation."
Annemarie Zielstra

Heli Tiirmaa-Klaar, Cyber Security Policy Advisor at the European External Action Service, touched on a related concern: "We need to ensure there is enough generalist knowledge [in companies] to facilitate the translation of the specific IT needs to the corporate board or high-level management."

One way of ensuring that cyber-related matters become established topics of boardroom discussions, in Neville-Jones's view, is to elevate the role of the Chief Information Officer within companies. "It does have an effect."

Zielstra explained the Dutch approach in convincing companies to devote adequate resources to cyber-security, through the concept of 'cyber-resilience'. "Cyber-crime for companies is all about business-continuity," she remarked. Should there be an incident or a spate of cyber-attacks, if businesses have taken the time to prepare themselves in advance, if they have already established systems for dealing with such matters, they can continue trading largely unaffected. It brings certainty and solidity to their operations, which can only encourage investors.

Zielstra's message to the business community is clear: "Cyber-resilience is not a technical issue, but a shared responsibility within the organisation." It must form part of any serious risk and reputation management exercise and should be the next new topic in companies' annual reports.

Neville-Jones concurred: "We need to get cyber-security into the risk register of companies." To

instigate these changes, she acknowledged that government has to provide sufficient leadership, which she believes it is doing.

"We decided that cyber-security was key to national security: it enables other forms of security to operate. Your defence is not going to operate unless your army's command core is hardened against attack. It's important to get national security defined in a broad sense."

She identified this approach as the principal reason why the UK treasury was persuaded to release €800million for cyber-security in 2010, at a time when nearly all other areas were facing cutbacks. "They realised that economic prosperity and future growth of economy and not just national security was dependent on cyber-security."

"They realised that economic prosperity and future growth of economy and not just national security was dependent on cyber-security."

Pauline Neville-Jones

The framing of the debate is crucial for an issue like cyber-security, which is still typically overshadowed by more conventional threats. Tiirmaa-Klaar highlighted this problem: "It's very hard at the national level to get money for the invisible issue of cyber-security. You don't see it when something blows up."

The second aspect to feature heavily in the debate was that of co-ordination and information-sharing. Lindberg used the attacks on Swedish IT service provider Tieto and the subsequent "severe co-ordination failure" as an illustrative example. She asserted that despite the medium-sized nature of the attack, the societal ripple effects were significant. "There were no joint processes in place for sharing information with all the stakeholders. It took weeks rather than hours to establish a situational overview."

"There were no joint processes in place for sharing information with all the stakeholders. It took weeks rather than minutes to establish a situational overview."

Furthermore, when it came to establishing priorities with regard to which services should be restored first, it was essentially in the hands of Tieto to decide. Hence, where governments have outsourced vital services to the private sector, there needs to be a clear set of guidelines for companies to follow in the case of a system failure. "The government can outsource services, but can never outsource responsibility to its citizens. When things go wrong, who will stand there?"

The subject of 'who dictates the priorities' in restoring services was picked up by Luukas Ilves, Head of International Cooperation at the Estonian Information Systems Authority. He highlighted the cross-dependencies between Estonia and Sweden.

"Our largest banks and telecommunications companies are Swedish." Consequently, Estonia enjoys excellent services in these sectors. Yet the companies naturally locate their internet servers in Sweden, explained Ilves.

"If service is interrupted, we suddenly don't have a vital service - banking." How can Estonia be sure

that the Swedish companies would give equal priority to restoring the Estonian parts of their businesses in the case of systemic meltdown? Ilves outlined three options for his country. The first would be to simply forbid companies from locating critical systems outside of Estonia.

The second would be to strike a bilateral agreement with the Swedish government, extracting guarantees that, in case of system failure, the restoration of services in Estonia would be on a par with the restoration of services to Sweden. Estonia would thus have to place a considerable amount of trust in the Swedish authorities.

The remaining alternative would be to conclude an agreement at the EU level and establish a truly single, consolidated market with standardised rules on such matters. Ilves hinted at his preference in his closing remarks: "We are not going to be able to regulate these things on a national level."

Moving on to the reporting of cyber-attacks, Merritt asked the participants how to get cyber-victims to talk more about incidents.

Neville-Jones expressed her concern that there is still "a reluctance to report". That is assuming that an organisation even knows that something has happened. She elaborated: "Many companies do not know that their intellectual property has been stolen. Awareness is a major issue." If firms do realise that there has been a breach of their IT system, they need to know *where* they should report it. Neville-Jones contended that, at present, most national police forces do not have sufficient capabilities in this area.

Lindberg advocated the creation of mandatory reporting systems, covering both the private and public sectors. She did not however favour reliance on the police in such matters and rejected the need to always launch criminal investigations as a matter of course so as to encourage cyber-victims to be more forthcoming.

"I would very much like to see a mandatory reporting system with anonymisation and not leading to a criminal investigation in every case."

Neville-Jones stated that such a mandatory reporting system to government would be useful, but insisted that this should not always lead to the information becoming public. In some cases, full

disclosure could be damaging and discourage future victims of cyber-crime from coming forward. She therefore favoured the selective use of "anonymisation" as a way to encourage organisations to provide more detailed accounts of any attack on, or breach of, their security system.

She underlined that there would still be certain consequences for businesses that operate with inadequate cyber-security protection: "Companies that deal in national security and allow breaches in their systems are unlikely to be hired. So there are business sanctions that apply."

The recourse to prosecution or punishment is thus not always necessary. She maintained that, "Transparency is a good hygiene instrument as it causes people to be careful. It brings about best behaviour."

There are, however, still certain misgivings within the private sector in relation to information-sharing. Cornelia Kutterer, Director of Regulatory Policy at Microsoft, expressed her organisation's view of the European Commission's existing framework.

"The Commission's current thinking on incident reporting does not encourage information-sharing. It's a one-way reporting scheme which does not enable enterprises to insert measures that are necessary."

By contrast, she commented that businesses are already sharing information on BotNet threats.

Zielstra remarked that it is imperative for CEOs to share lessons learned with other CEOs to help improve cyber-resilience across the board. With this in mind, when the Dutch government set up a National Infrastructure against Cyber Crime (NICC) in 2006, it also established information-sharing partnerships (ISACs) between the public sector and thirteen industrial sectors, which operate on a voluntary basis but with certain obligations attached.

"When there is trust, you can share information," she explained. The scheme emphasises the need for all stakeholders to hold regular face-to-face meetings so that trust can be developed over time.

Neville-Jones agreed, adding that it is important for enterprises to feel that they are on safe territory when sharing information with competitors. She underlined the need for an international legal framework whereby companies can share cyber-security related information without the fear of falling foul of anti-trust legislation.

"In the U.S., the anti-cartel legislation is much more severe than in Europe." This could pose a problem for many, particularly for European firms with a sizeable presence in the American market. Neville-Jones's opinion was that the unnatural and usually undesirable tendency for rival firms to help each other out needs to be reversed to effectively address the collective cyber vulnerabilities.

"We've grown up in a need-to-know context for security, and need-to-know still has its place, but we now need a need-to-share." Whether anonymisation proves to be an effective way of promoting this, remains to be seen.

A further concern was put forward by Nicole Dean, Director of Cyber Programs at Raytheon. She first put the challenge into perspective by stating that "we have to reach everybody" then posed the question: "How do we institutionalise cyber-security and not make it compliance based?"

In her opinion, existing regulations have the tendency to become little more than box-ticking exercises for firms. "We need a whole mentality shift. A conversation between industry and government is the only way to achieve cyber-security."

Neville-Jones re-emphasised the point: "We need not just coordination but *partnership* between the public and private sectors."

"The threats these days are not just to the state and its institutions, but to the well-being of society as a whole and the functioning of the economy."

"The threats these days are not just to the state and its institutions, but to the well-being of society as a whole and the functioning of the economy."

Pauline Neville-Jones

Given the all-encompassing nature of the threat, the panellists were united in reinforcing the message that, to significantly reduce vulnerability to cyber attacks, all of society has to be actively involved.

List of participants

Eda Aygen
Project Manager
Security & Defence Agenda (SDA)

Jakub Boratynski
Head of Unit, Fight against organised crime
Directorate General for Justice, Freedom and Security, European Commission

Gabriele Borla
Head of Unit, Infrastructure
European Defence Agency (EDA)

Nicole Dean
Director of Cyber Programs
Raytheon

Adele Folletti
Security Practice Director
Bull

Brigid Grauman
Independent journalist

Andrea Ghianda
Project Manager
Security & Defence Agenda (SDA)

Luukas Ilves
Head of International Cooperation
Estonian Information Systems Authority

Cornelia Kutterer
Director of Regulatory Policy
Microsoft

Helena Lindberg
Director General
Swedish Civil Contingencies Agency

Giles Merritt
Director
Security & Defence Agenda (SDA)

Sara Myrdal
Principal Analyst
Swedish Emergency Management Agency (SEMA)

Baroness Pauline Neville-Jones
Special Representative to Business on Cyber Security
Cabinet Office, United Kingdom

Detlef Puhl
Senior Advisor, Strategic Communications
Emerging Security Challenges Division
NATO

Sue Roddy
Director
Unified Cross Domain Management Office, US Department of Defense

Jonathan Sage
Government Programmes Executive
IBM UK

Brooks Tigner
Editor
Security Europe

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

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

Wout Van Wijk
Public Affairs and Communications Manager
Huawei Technologies

Etienne Verhasselt
External Counsel
PwC

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

Upcoming events

Cyber-initiative

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

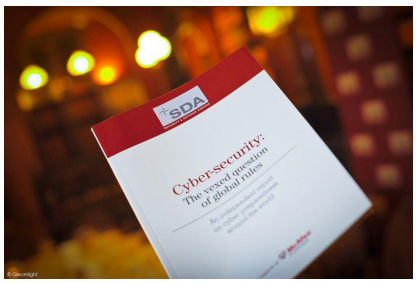
It will seek to examine global governance matters such as the application of international law on cyber-space, EU-US cooperation, as well as building confidence and trust between different stakeholders. The initiative will analyse horizontal policy issues such as resilience, skills, training and education.

Past cyber-initiative speakers & topics

The 2012 saw the first year of the SDA's cyber-security initiative, which concentrated on defining cyber-security and the most prominent threats, as well as the interactions between the private and public sectors.

The evening and dinner debates evolved around topics such as international responsibility, information and intelligence sharing, prevention and resilience, cyber-preparedness in EU states and legislative proposal of the EU, protection of critical infrastructure as well as public-private partnerships.

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



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

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

SECURITY & DEFENCE AGENDA (SDA)

Bibliothèque Solvay, Parc Léopold, 137 rue Belliard, B-1040, Brussels, Belgium
Tel: +32 (0)2 737 91 48 Fax: +32 (0)2 736 32 16 E-mail: info@securitydefenceagenda.org

www.securitydefenceagenda.org
@secdefagenda