The European Security Round Table

debates ★ analysis ★ policy support

European Security Round Table (ESRT)

&

Estonian Ministry of Defence

co-organised

European Cyber Security Conference

Shared Threats – Shared Solutions:
Towards a European Cyber Security Policy

Tuesday, 14 June 2011
Charlemagne Building
European Commission
Brussels

realised in cooperation with:

SAP®

CASSIDIAN
AN EADS COMPANY

SRA INTERNATIONAL, INC.

European Cyber Security Conference

Shared Threats – Shared Solutions: Towards a European Cyber Security Policy

The Ministry of Defence of Estonia, together with the European Security Round Table, organized on 14 June 2011 a high-level cyber security conference hosted in the European Commission's Charlemagne Building in Brussels. The event gathered together around 120 participants from the EU institutions, Member States, NATO and industry. Over the course of the day's events, a broad range of issues relating to cyber security and the international coordination of policy were discussed. The conference was moderated by Christoph Raab, director of the ESRT.

Opening the conference was a keynote address by the Minister of Defence of Estonia, Dr. Mart Laar, who stressed the importance of cooperation, both internal and external, in the coordination of cyber security. The Minister demonstrated that old dividing lines (between defence and security, law enforcement and military, public and private, etc.) do not hold in cyberspace; therefore, governments need to coordinate activities across ministries and departments using broad national cyber security strategies and appointing lead agencies or individuals. Also, it would be essential for governments to cooperate with the private sector, as the majority of web infrastructure is in private hands. Yet deepening international cooperation is just as important a goal. The Minister invited countries to exchange information and analysis on cyber attacks and to harmonize legal definitions and humanitarian law for cyber conflicts, while also stressing the need for countries to join the Council of Europe's Convention on Cyber Crime. Cyber security begins at the homes of Internet users; good cyber citizenship and cyber hygiene are of the utmost importance.

Dr. Laar also pointed out some practical proposals to help European actors create a safer cyber space. First among these was the importance of ensuring that national and EU institutions' networks are secure and have not been penetrated. The EU's cyber activities need to be better coordinated on both the institutional and member state levels. The EU should focus on areas where it has particular competence, such as protecting critical infrastructure and coordinating legal structures, as well as regulating and working with business, consumer protection and privacy, and anti-terrorism. The EU's Common Foreign and Security Policy (CFSP) would be needed to extend Europe's cyber security agenda across the globe, which would in turn stress to developing countries that cyber security is compatible with individual rights, privacy and free speech. The Minister also found that Common Security and Defence Policy (CSDP) could be used for furthering the EU's cyber agenda; CSDP must ensure that forces on EU military operations and


civilian missions are protected against cyber attacks. Cyber defence should be made an active capability of CSDP; it is crucial that the EU take advantage of the overlaps it shares with NATO to coordinate activities between the two organisations.

The European Keynote was delivered by the EU Commissioner for Home Affairs, Mrs Cecilia Malmström. The Commissioner noted the current fragmentation of European cyber policy and the need to overcome it. She stressed that cyberspace is not so different from the traditional spaces of social interaction, and that threats in cyberspace are very real. The number of cyber attacks in the world is constantly growing and so is the cost of cybercrime. Also, the EU institutions are far from immune. Recent cyber attacks on EU IT infrastructure sped up the creation of the Computer Emergency Response Team (CERT) for the European Institutions, which is active from the beginning of June this year. The Commissioner underlined the importance of joining forces in the EU if we intend to successfully fight cyber-criminals and strengthen the security of EU networks. She recalled different policy approaches, including the EU Internal Security Strategy adopted last year, which lists cybercrime and cyber security high on the list of security challenges. She also stressed the importance for Member States and EU institutions (as well as the public and private sectors) to work together in capacity building in law enforcement and the judiciary, as well as training and dealing better with cyber attacks. Commissioner Malmström announced the establishment of a European Cybercrime Centre by 2013, for which a feasibility study has already been launched. She also noted that citizens and companies must be encouraged to report crimes more often, since crimes cannot be solved if they are not reported in the first place. Cybercrime is a global problem and, therefore, needs a global response. The EU is working closely with the US in this matter and contacts have been established between the EU and NATO. Finally, the Commissioner urged Member States who have not already done so to speed up efforts to join and ratify the Council of Europe's Convention on Cyber Crime.

> *"Cyber security is compatible with individual rights, privacy and free speech."*

Panel Session I – Cyber Security – the Case for European and International Coordination

The panel was chaired by **Christian Jechoutek** (Assistant Director, Capabilities Department, Europol) and speakers included **Richard Wright** (Director Conflict Prevention and Security Policy, EEAS), **Gábor Iklódy** (Assistant Secretary General, NATO), **Oliver Rüss** (Advisor to the European Counter Terrorism Coordinator), **Mike StJohn-Green** (Deputy Director, Office of Cyber Security and Information Assurance, Cabinet Office, UK)




and **Eric Windmar** (Cabinet Cecilia Malmström, European Commission).

The introductory remarks highlighted the financial damage on society that is regularly caused by software viruses and cyber attacks. Nearly 6% of European bank accounts have been subject to internet fraud, and as cloud computing is becoming more popular its attractiveness to criminals is on the rise as well. Furthermore, cyber security can be linked with counter-terrorism, as terrorists are increasingly keen on using new technologies in cyber space. A holistic approach including civil-military cooperation and public-private partnership needs to be applied for a more secure cyber space as well as to counter terrorism.

> *"A holistic approach including civil-military cooperation and public-private partnership needs to be applied for a more secure cyber space as well as to counter terrorism."*

Several speakers stressed the importance of actions on all fronts, internally as well as externally. A coordinated approach is needed between different organizations and other actors. On the EU side, the newly created European External Action Service foresees three work strands in the area of cyber defence: 1) promoting dialogue with partners such as the US, India, NATO, as well as the private sector; 2) promoting capacity building in third world countries and supporting their adhesion to the Budapest Convention; 3) working on strategy. Cyber attacks can be a threat to EU military operations, and the updated European Capabilities Development Plan lists Cyber Defence as one of the ten priority areas in capability development. The EU is also making efforts to coordinate actions between the different COM DG-s in order to ensure their complementarity.

NATO is focusing on cyber defence rather than cyber security. Cyber attacks are regarded by the Alliance as one of the most serious security concerns, as around 70% of all information generated is exchanged through the Internet. The range of cyber attacks has increased, including wide-scale disruptions. NATO adopted its first cyber defence policy in 2008, with the main purpose of protecting its own networks. The Lisbon Summit in 2010 was the first time that cyber attacks were viewed in the context of collective defence, and in June 2011 a reviewed cyber defence policy and action plan were adopted. The reviewed policy goes beyond protection of NATO's own networks and identifies three layers: 1) protection of NATO networks - a centralised fully operational capability should be in place by the end of 2012; 2) minimum requirements for national Command and Information Systems, which are connected to NATO CIS; 3) protection of national critical infrastructure and reducing existing vulnerabilities. The latter is an area where



NATO can assist, but essentially the task remains the individual nation's own responsibility. NATO also stresses the importance of partnerships, as private companies, civil and other important actors do not fall under the alliance's competency.

The panel pointed out that Member States have a different level of awareness regarding cyber threats. Also in terms of countering those threats, some are quite advanced in their technological competence as well as internal structures, while others are much less so. Raising public awareness of cyber threats and the need to invest money in developing measures for protection is something that all countries could improve upon. In terms of norms and regulations, countries are advised to envision and describe their future security environment, which is where the EU could help as well.

> *"Overall, cyber security should not be seen as a NATO or an EU issue but rather as a national issue, and various instruments available within the NATO and EU framework should be used in a coordinated way."*

Overall, cyber security should not be seen as a NATO or an EU issue but rather as a national issue, and various instruments available within the NATO and EU framework should be used in a coordinated way. NATO concentrates on defence and has a unique operational capability, while the EU has the regulatory instruments and is in a better position to implement the civil-military approach. While contacts between NATO and EU in that area already exist, it would be beneficial to strengthen them and increase cooperation.

The **NATO keynote, presented by Lt. Gen. Kurt Herrmann, Director of NATO Communication and Information Systems Services Agency (NCSA)** focussed on the operationalisation of NATO's cyber defence policy. He presented an overview of the outcomes of NATO's Lisbon Summit of 2010 vis-à-vis cyber defence, as well as stressing the importance of cyber security in today's world of interconnected networks where effective collaboration between partners is crucial. Lt. Gen. Herrmann also explained the different roles of NCSA and reaffirmed that there has always been close cooperation with industry. Furthermore, on the operational side, first contacts have also been established with the EU Commission. The NATO keynote was followed by **a demonstration cyber security exercise by Col. (Ret.) Jon Noetzel of SRA**, who gave an impressive account of how a lack of information exchange between Member State agencies can be a substantial weakness for the EU. Afterward, a **keynote speech by Prof. Udo Helmbrecht, Director of ENISA,** was delivered on




the Agency's role in securing Europe's information society. Dependency on IT is growing rapidly and so is the effectiveness of malware. Prof. Helmbrecht gave an overview of ENISA and its activities in this environment, of which the main strands are advising and assisting the Commission and the Member States on information security, collecting and analyzing data on security practices in Europe and emerging risks, and promoting risk assessment and risk management methods as well as awareness-raising and cooperation between different actors in the information security field. Facilitating public-private partnership is of utmost importance and three working groups have been established to discuss related issues. Prof. Helmbrecht also touched upon Pan-European exercises and goals for the European CERT programme.

> *"To achieve this cooperative atmosphere, a precondition of mutual trust between stakeholders has to be met."*

Panel Session II – Cyber Security and Critical Information Infrastructure Protection (CIIP)

This panel was chaired by **Luigi Rebuffi,** CEO of European Organisation for Security, and speakers included **Andreas Könen** (Federal Office for Information Security, Germany), **Robert G. Bell** (Senior Civilian Representative of the Secretary of Defence, Europe and Defence Advisor to the US Ambassador to NATO), **Christian Ehler** (MEP, Rapporteur for ENISA), **Antti Ilmari Peltomäki** (Deputy Director General, DG INFSO) and **Brig. Gen. Jon Mullin** (Capabilities Director, EDA). The session was preceded by an **industrial keynote by Mr. Hervé Guillou, CEO of Cassidian Systems.** Mr. Guillou stated that a lack of coherent legal framework is an obstacle in organising the fight against cyber crime (for instance, in the US cyber crime can be considered an act of war, yet in other countries it is not considered a crime). He also advocated a common normative framework and common standards, and creating trusted partnerships between the private and public sectors.

In Panel II, speakers acknowledged that information systems and networks are exposed to an ever-growing number and range of threats and vulnerabilities. They also highlighted the relevance of strengthening EU wide cooperation, including cooperation between Member States' CERT-s to provide protection for CIIP. In addition, the private sector should be encouraged to invest in cyber security. To achieve this cooperative atmosphere, a precondition of mutual trust between stakeholders has to be met. It was mentioned that only 9 out of 27 Member States of the EU have adopted a national cyber security strategy in spite of the growing number of threats and risks. In particular, the panel was critical of the political blockages that have held up internal

NATO negotiations on cyber policy, and doubt was expressed that the EU and NATO would easily come to an agreement, given the divisions inside NATO itself. It was also argued that the vague wording often used to achieve consensus would not result in the establishment of effective policy.

The importance of the 2009 CIIP Action Plan and the Commission's 2nd Communication on Critical Information Infrastructure Protection from March 2011 were mentioned; further activities on the European level are also to be guided by EU Internal Security Strategy and the Digital Agenda for Europe. It was acknowledged that a coherent approach is still lacking on national, international and European levels, and that ENISA has an important role to play in building up expertise in network information and cyber security while supporting cooperation between Member States and other stakeholders. ENISA could also play a key role in more substantive preventive action and raising awareness of cyber threats. In addition to reinforced cooperation across countries and across sectors, the panellists found it important for the EU to cooperate with NATO, since cyber threats do not recognize organisational boundaries. There is great potential for the two organizations to work together. Cyber security is very much a civil-military area: now that both parties use the same technologies, cyber issues should be dealt with holistically. There is a much greater need to share information and the European Defence Agency is cooperating with the ACT specifically on the conceptual side.

> *"A public-private dialogue can be very powerful and is very important, albeit right now there still remains fragmentation."*

The 2nd panel session was followed by a **moderated discussion: Strong Partnerships between Governments and Private Sector – a Way to Foster Security in Cyberspace** (moderator Luigi Rebuffi) with speakers **Mário Campolargo** (Director Emerging Technologies & Infrastructures, DG INFSO), **Julio Martinez Meroño** (Member of Cabinet, Secretary of State, Ministry of Interior, Spain), **Sean O'Brien** (Vice President (Global) Public Safety & Security SAP) and **Heli Tiirmaa-Klaar** (Cyber Defence Policy Advisor at NATO). It was emphasized that a public-private dialogue can be very powerful and is very important, albeit right now is hindered by fragmentation. We should focus on how to respond to a cyber attack and maintain the level of service we are used to. An effective public-private partnership (PPP) should mean sharing and setting boundaries in a way that lets business innovate. At the same time a clear distinction should be made regarding what the role for the public sector is. This can be anywhere from the role of facilitator to providing a good platform to make direct investments. The role of the private sector is to cooperate with the public sector and create the necessary trust in the


government. It is also worthwhile to look into the private-private partnership model. It was underlined that the Commission gives a great deal of funding to PPP and that the key point is not just to be reactive, but proactive in order to have an impact on the perception of cyber space. A conclusion can be drawn that PPP already exists but that there is a need to further deepen the dialogue.

The concluding remarks of the Conference were made by Ambassador Jüri Luik, Permanent Representative of Estonia to NATO. The Ambassador warned that large cyber attacks are still waiting for us and that we should prepare ourselves. In contrast to 9/11, our current understanding of cyber attacks is much better than was our understanding of the scope of terrorism before the attacks on the twin towers. Drawing from the discussions of the day, he emphasized that in order to combat the growing number of cyber threats actions are needed on all fronts, both externally and internally, on a state and cross-organizational as well as citizen level. An appropriate involvement between public and private sectors needs to be identified. Furthermore, cooperation should not only be institutionalized but should also take place between experts based on good personal contacts and networking.

Ambassador Luik pointed out that a number of EU initiatives are already in place; however, he argued that better cooperation is needed, including with NATO. The two organizations should work in cyber security as closely as possible, but they have somewhat different approaches. Also, in the EU there is such a wide arrangement of agencies dealing with cyber issues that is it hard to pinpoint a single partner for NATO. The EU is in a better role to implement a holistic approach on cyber security; it is a role for civilian agencies and the EU in particular to work on the protection of CIIP. A comprehensive "whole-of-the-Union" policy approach to cyber security among EU institutions is needed to deliver real, tangible improvements to cyber security, both for the institutions and the Member States. CFSP should be used to share competences and knowledge on cyber security with EU partners and outreach countries. Integrating CFSP with EU assistance programs could help resource-constrained nations develop their own capabilities.

Overall, the conference provided an interesting platform for the subject of cyber security and its integration into the EU. It is clear that there remains a large amount of fragmentation between the various agencies and levels of government, and resolving this fragmentation is of the utmost importance. In addition, developing channels to integrate private companies with the public sector will help build better lasting networks and solutions. The issue of cyber security continues to be a pressing one, and the ESRT and the Estonian Ministry of Defence intend to continue this series of discussions. Also, the ESRT will organise a **cyber security event targeted to MEPs in November**.


Dr. Mart Laar
Minister of Defence of Estonia

Ambassador Jüri Luik
Permanent Representative of Estonia to NATO

Organisers

Kai-Helin Kaldas
Counsellor for CSDP
Estonian EU Representation

Christoph Raab
Director of European Security Round Table

Contact:

Estonian Ministry of Defence
Sakala 1, 15094 Tallinn, Estonia

Phone: +372 717 0022
E-mail: info@kmin.ee

Permanent Representation of Estonia to the EU
Rue Guimard 11/13, 1040, Brussels, Belgium

Phone: +32 2 227 39 10
Press: +32 2 227 39 22

Email: permrep.eu@mfa.ee

Project Management Team:

- Andy Stirnal
- Wiebke Miara
- Paul Tuthill
- Gregory Irwin

Contact:

European Security Round Table sprl
Cours St. Michel 100/1
1040 Bruxelles, Belgium

Phone: +32 2 640 63 92
Fax: +32 2 646 61 93

info@security-round-table.eu
http://www.security-round-table.eu