CONFRONTING CYBERTERRORISM: TACKLING POLITICAL ASPECTS OF CYBERSECURITY

International conference and expert workshop organized by the Association for International Affairs in cooperation with the U.S. Office of Naval Research Global, the Estonian Embassy in Prague and the North Atlantic Treaty Organization Public Diplomacy Division

December 6-7, 2011
Venue: The European Commission Representation in the Czech Republic, Jungmannova 24, Prague 1

Asociace pro mezinárodní otázky
Association for International Affairs

Synopsis

Cybersecurity has recently become a much debated issue. After the attacks on Estonia and Georgia, the topic gained broad attention and, subsequently, was elevated to the very top of agendas of the Euro-Atlantic security organizations (including the 2008 Report on the Implementation of the European Security Strategy and the 2010 NATO Strategic Concept) and their member states (as documented by recent releases of cybersecurity strategies in the United States, Great Britain or Germany).

The issue of cybersecurity turns out difficult to be comprehensively managed, as it covers many different, seemingly disparate areas – information technologies, domestic and international law, intelligence, military and defence issues, politics and international relations. On the other hand, this is hardly a completely new situation: During the past decades, states have been confronted with various security threats which defied neat compartmentalization and required a complex, multi-institutional and cross-border approach (with terrorism serving as an instructive example).

The issue of cybersecurity can be divided into three broad areas: The first comprises attacks against critical parts of defense infrastructure and can be described with the traditional vocabulary of intelligence and warfare. The second area represents an 'outreach' of organized crime, and comprises profit-oriented illicit activities in the cyberspace. Last but not least, cyber-activities include politically motivated attacks where the IT and other infrastructure only serves as the 'first target', a tool to influence the 'second target' which is the population and its political representation – cyberterrorism, to use a concise term for a complex fact.

The planned international conference and expert workshop intend to focus on the latter aspect of cybersecurity, for two main reasons. Firstly, in the context of Central and Eastern Europe, politically motivated cyber-attacks seem to represent the most pressing issue, as the cases of Estonia and Georgia aptly demonstrate. Secondly, unlike cyber-crime which tends to be dominated by legal issues (apart from the apparent technological component), cyberterrorism has the potential of connecting experts from many different fields, including IT specialists, lawyers, politicians, security and defense experts. A workshop focusing on this issue displays an especially rich potential for cross-fertilization and creating new functional links.

The conference will thus primarily focus on the complexity and problems of the decision-making process in reaction to politically motivated cyberattacks, taking into account its multiple dimensions, from the technical through legal to political aspects and international cooperation. The main objective of the conference and workshops is to improve expert understanding of specific aspects of cybersecurity among relevant experts in the regional, European and Euroatlantic contexts. It also aims at promoting exchange of ideas and creating personal links across different institutions and disciplines and overcome the divide between technical and social aspects of cybersecurity. Finally, we strive to educate broader public about the issue which has consistently risen as a security concern and challenge.

Tomáš Karásek
Director, Research Center of the Association for International Affairs

Workshop Proceedings

The discussion is based on a fictional scenario of a series of cyber attacks. The scenario tries to capture some of the recent experiences in several countries, but also future cyber threats as articulated by security experts.

The scenario is divided into different phases, parts and sub-parts. In each phase, a series of events are presented, followed by detailed issues.

As a particular event is introduced, members of the audience are expected to familiarize themselves with the event displayed, and thereafter offer observations, opinions and solutions.

The emphasis of the discussion should be on issues related to decision-making at the grand strategic and strategic levels of government. In analyzing particular events, it aims to address, among others, the **following questions**:

- What decisions should be taken in order to effectively respond to the situation, event or issue presented?
- Who should be responsible for taking decision(s)?
- What information is needed for taking decision(s)?
- With whom should the information on a particular event or issue be shared?
- What is the applicable regulatory framework?
- What resources are required?
- What possible conflicts of interest between various groups of interest may arise?
- What additional information is required for effective decision-making?

The purpose of the discussion is not to find technical solutions, devise technical responses to a particular form of cyber attack. The goal is to hold a discussion on strategic implications of a cyber attack. If certain technical terms used need to be explained, do not hesitate to ask. However, the discussion should not span around the possibility/impossibility or technical execution of a particular event. For the purposes of this discussion, the participants have to assume that all attacks, responses and other technical activities described are possible and validated.

The discussion is moderated. Moderator has the right to end a particular discussion or to issue “rulings” if this is necessary for the facilitation of the debate.

Disclaimers:

- The countries and their names used are fictional. None of the countries used in the scenario corresponds to a particular country.
- The laws and regulations of a country called “Homeland” in the scenario are assumed to be those of the Czech Republic.
- The scenario to be discussed is unclassified but it is not meant for publication.
- The scenario to be discussed is copyright protected with the European Cyber Security Initiative, Tallinn, Estonia. No part of this material may be copied or reproduced without the express written approval of the European Cyber Security Initiative.

Programme

December 6-7, 2011
Venue: The European Commission Representation in the Czech Republic, Jungmannova 24, Prague 1

December 6, 2011 - International Conference

14:00 - 14:30 **REGISTRATION**

14:30 - 15:00 **OPENING SESSION**

Welcome Remarks:
Maria Staszkiewicz, Director, Association for International Affairs, Czech Republic
H. E. Norman Eisen, Ambassador of the United States of America to the Czech Republic
H. E. Lembit Uibo, Ambassador of Estonia to the Czech Republic

15:00 - 17:00 **PANEL DISCUSSION – POLITICAL ASPECTS OF CYBERSECURITY: RECENT DEVELOPMENTS AND FUTURE CHALLENGES**

Keynote Speech:
Ilmar Tamm, Director, Cooperative Cyber Defence Centre of Excellence, Estonia

Chair:
Tomáš Karásek, Director of the Research Center, Association for International Affairs, Czech Republic

Discussants:
Eduardo Gelbstein, Adjunct Professor, Webster University, Senior Fellow, Information Management and Security, Diplo Foundation, Switzerland
Paul de Souza, Director, Cyber Security Forum Initiative – Cyber Warfare Division, USA
Eneken Tikk, Independent Legal and Policy Analyst , Estonia
Rodica Tirtea, Expert, European Network and Information Security Agency, Greece

18:00 - 20:00 **RECEPTION (special invitations only)**

Venue: Embassy of Estonia, Na Kampě 498/1, Prague 1

Programme

December 7, 2011 - Expert Workshop (special invitations only)

10:00 - 11:30 **RESPONDING TO A POLITICALLY MOTIVATED CYBERATTACK: NAVIGATING THROUGH THE DECISION-MAKING MAZE – PART I**

Chair:
Lauri Almann, President, European Cyber Security Initiative, Estonia

11:30 - 12:00 **COFFEE BREAK**

12:00 - 13:30 **RESPONDING TO A POLITICALLY MOTIVATED CYBERATTACK: NAVIGATING THROUGH THE DECISION-MAKING MAZE – PART II**

Chair:
Lauri Almann, President, European Cyber Security Initiative, Estonia

13:30 - 14:30 **BUFFET LUNCH**

14:30 - 16:30 **LESSONS LEARNED: COMPLEXITIES AND CHALLENGES OF RESPONDING TO CYBERTERRORISM – FINAL ROUNDTABLE**

Chair:
Tomáš Karásek, Director of the Research Center, Association for International Affairs, Czech Republic

Speakers

Lauri Almann

Lauri Almann is President of the European Cyber Security Initiative, a Tallinn-based NGO. He has MA in International Law from the Georgetown University Law Centre, USA. Prior to joining the private sector, for 10 years he had worked in various top-level civil service positions, including a position of a Permanent Undersecretary at the Estonian Ministry of Defence, Legal Counsel and Advisor to the Minister of Defence and a diplomat in several Estonian diplomatic missions abroad. Mr Almann was a part of the team that organized the response to the cyber-attacks on Estonia in 2007 and participated in the establishment of the NATO Cooperative Cyber-Defence Centre in Tallinn. He contributed to the drafting of several legal acts, including the Public Information Act and the National Defence Act. Mr Almann regularly publishes articles, delivers speeches and participates in various public initiatives on cyber security.

Norman Eisen

H.E. Norman L. Eisen is the United States Ambassador to the Czech Republic. He holds his B.A. from Brown University and J.D. from Harvard Law School. After having practised law for 18 years, he joined then-President-elect Barack Obama transitional team. In 2003, he co-founded a government watchdog organization the Citizens for Responsibility and Ethics, Washington, that targets corrupt officials. In 2009, Mr Eisen was named Special Counsel for Ethics and Government Reform. Before starting to work on ethics reform, Mr Eisen also worked on education policy.

Eduardo Gelbstein

Eduardo Gelbstein is currently Adjunct Professor at the postgraduate Business and Technology Department of Webster University and Senior Fellow of the Diplo Foundation. He has extensive experience in the information security area, having worked for the United Nations Board of Auditors, the The Court of Accounts in France, UN International Computing Centre and having been a member of the Information and Communications Task Force set up by the UN Secretary General, Kofi Annan. Dr Gelbstein has run workshops on information security, cyber-terrorism and cyber-war at the United Nations in New York since 2001 as well as workshops on best practices in IT for numerous organizations around the world. He is a regular speaker at international conferences and the author of many publications, such as the book ‘Information Insecurity’ (2002) and ‘Cyber-Terrorism, Cyber-War and Digital Immobilisation’ (to be published in 2012) which he co-authored.

Tomáš Karásek

Tomáš Karásek is Director of the Research Center in the Association for International Affairs. He is responsible for the management of its research and publication activities, and coordination of the team of AMO analysts. He earned his master degree and Ph.D. in International Relations at the Faculty of Social Sciences, Charles University in Prague (where he also graduated from the Law Faculty). Since 2004 he has been a lecturer at the Faculty’s Department of International Relations. He has been actively involved in research activities and has coordinated several grants on the topic of European security. In 2009 he spent his sabbatical in Shanghai where he taught at the Fudan University. From September 2009 to June 2010 he was a Fulbright scholar at the Saltzman Institute of War and Peace Studies, Columbia University in New York.

Speakers

Ralph Lüftner

Ralph Lüftner is Product Manager for the security appliance SCALANCE and communication processor CP443-1 Adv with built-in security features at Siemens. He has been with the company for 10 years now, having done field-services for industrial communication systems, consultancy for Industrial IT-security and worked at the Development of Siemens Industrial Communication unit. Simultaneously, Mr Lüftner has been teaching at the Siemens SITRAIN, carrying out workshops and courses for customers (basic industrial Ethernet, basic PROFINET and basic Security), and occasionally at the Siemens Technik Akademie teaching Industrial Communication.

Paul de Souza

Paul de Souza is Founder and Director of the Cyber Security Forum Initiative (CSFI) and its divisions CSFI-CWD (Cyber Warfare Division) and CSFI-LPD (Law and Policy Division). He has over 12 years of cybersecurity experience. He worked as Chief Security Engineer for AT&T, where he designed and approved secure networks for MSS. Mr de Souza also served as Security Engineer for CSC and US Robotics. He has consulted for several governments, military organizations, and private institutions on best network security practices and also presented in Estonia, Georgia, Australia, and all across the United States.

Ilmar Tamm

Col. Ilmar Tamm is Director of the Centre of Excellence of the Cooperative Cyber Defence in Estonia. He graduated from the Finnish Military Academy, finished Staff Officer training at the Estonian National Defence College and Senior Staff Officer Course at the Finnish National Defence College and attended Signal Officer Basic Course in Fort Gordon, the US Army Signal Centre in Georgia. He served as Chief of Communication and Information Systems Department (J6) of the Estonian Defence Forces. During his assignment at the Allied Land Component Command Headquarters in Heidelberg, Germany he spent 6 months in Afghanistan serving as a Chief of Operations of the CJ6 Joint CIS Control Centre (JCCC).

Eneken Tikk

Eneken Tikk-Ringas holds a doctor juris degree from the Tartu University, Estonia since 2011. During her studies in Estonia, Sweden, Finland, Germany and the United States she has conducted extensive research in the field of IT and law, including data protection, electronic communications, cyber security and cyber defense. Currently working as an independent expert, Dr Tikk-Ringas served as legal adviser and acting head of the Legal and Policy Branch at NATO Cooperative Cyber Defence Centre of Excellence, Tallinn in 2008-2011. Her previous assignments included heading the Estonian MOD's Cyber Defence Legal Expert Team tasked with the analysis of Estonian cyber security law in response to 2007. Before this, she was in charge of developing the legislation for Estonian access to Schengen area at the Estonian Ministry of Justice. Ms Tikk-Ringas has also an extensive teaching experience (e.g. with Swedish National Defense College, Tallinn Technical University, Tartu University, Estonian Business School, Estonian Academy of State Defence and Estonian Military Academy). She has published numerous articles and books in the field.

Speakers

Lembit Uibo

H.E. Lembit Uibo is Ambassador of the Republic of Estonia to the Czech Republic. He graduated from the Estonian School of Diplomacy and holds M.A. in International and European Relations from Amsterdam University and M.A. in European and Comparative Law from Maastricht University. During the Estonia's EU accession process, Mr Uibo worked at the Foreign Ministry's European Union law division, consulting law-related accession negotiations with the EU and preparing the Accession Treaty. Mr Uibo also served as Counsellor to the EU law division, Director of the Foreign Ministry's European Union Court division and was the Estonian representative to the European Court of Justice.

Michael W. Weir

Michael W. Weir is Senior System Architect and Analyst at Quanterion Solutions, Incorporated, Utica, USA. His responsibilities cover technical lead for the Defense Technical Information Center (DTIC) Data and Analysis for Software (DACS), providing insight and innovation to the DACS team transitioning from a document-focused repository to an on-line information sharing community. Prior to the Quanterion Solutions, Mr Weir served as Chief of Communications and Information Systems for Eastern Air Defence Sector, Senior System Engineer for Oasis Systems, Inc. and SI International. He was a member of initial cadre tasked to develop and implement the first Defensive Information Warfare component at the Air Force Research Laboratory in the USA. He is also President of the Information Systems Security Association (ISSA).

Team

Tomáš Karásek

Director of the Research Center
Association for International Affairs

Maria Staszkiewicz

Director
Association for International Affairs

Tereza Jermanová

Conference Service
Association for International Affairs

Vlaďka Votavová

Executive Secretary
Association for International Affairs

Zuzana Bartková

Secretary of the Research Center
Association for International Affairs

Conference Staff, Association for International Affairs:
Vendula Filipová, Bettina Molnárová, Michaela Očková, Lilia Revak, Ondřej Srb, Jakub Záhora

We would like to thank all those whose help and cooperation have made this event possible.

Association for International Affairs

Association for International Affairs (AMO) is a preeminent independent think-tank in the Czech Republic in the field of international affairs and foreign policy. The mission of AMO is to contribute to a deeper understanding of international affairs through a broad range of educational and research activities. Today, AMO represents a unique and transparent platform in which academics, business people, policy makers, diplomats, the media and NGO's can interact in an open and impartial environment.

IN ORDER TO ACHIEVE ITS GOALS AMO STRIVES TO:

- formulate and publish briefings, research and policy papers
- arrange international conferences, expert seminars, roundtables, public debates
- organize educational projects
- present critical assessment and comments on current events for local and international press
- create vital conditions for growth of a new expert generation
- support the interest in international relations among broad public
- cooperate with like-minded local and international institutions

RESEARCH CENTER

Founded in October 2003, the AMO's Research Center has been dedicated to carrying out research and raising public awareness of international affairs, security and foreign policy. The Research Center strives to identify and analyze issues important to Czech foreign policy and the country's position in the world. To this end, the Research Center produces independent analyses; encourages expert and public debate on international affairs; and suggests solutions to tackle problems in today's world. The Center's activities can be divided into two main areas: First, the Center undertakes research and analysis of foreign policy issues. Second, the Center fosters dialogue with the policy-makers, expert community and broad public.

Asociace pro mezinárodní otázky
Association for International Affairs
www.amo.cz

Notes

Organizer

Asociace pro mezinárodní otázky
Association for International Affairs

Partners

Office of Naval Research
USN GLOBAL
Science & Technology

Estonian Embassy in Prague

NATO OTAN

EurActiv.cz
Vaše internetová brána do Evropy

Association for International Affairs (AMO)
Žitná 27
CZ 110 00 Praha 1
Tel/Fax +420 224 813 460
info@amo.cz
www.amo.cz