enisa

2nd International Conference on Cyber-crisis Cooperation and Exercises

23-24 September 2013
Athens, Greece

Participant information package

enisa

www.enisa.europa.eu

Foreword by the ENISA Executive Director

Prof. Dr. Udo HELMBRECHT
Executive Director of ENISA

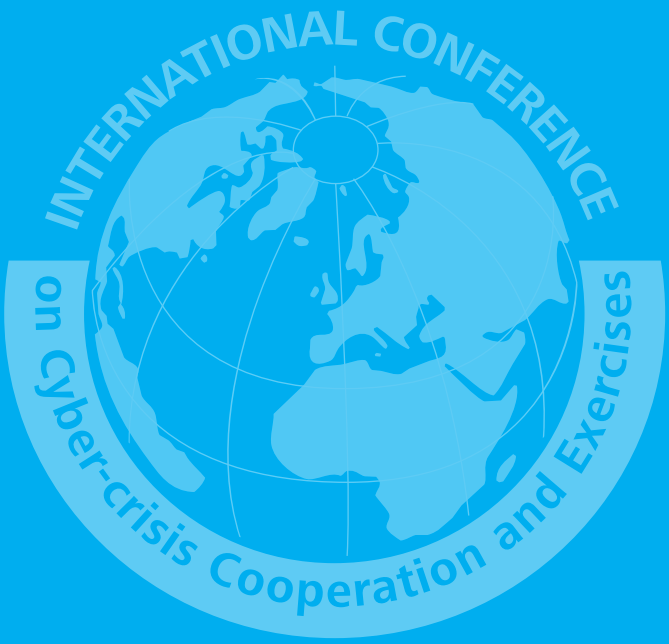
It is my great pleasure to welcome you all to our 2nd International Conference on Cyber Crisis Cooperation and Exercises, this year taking place in Athens, Greece. Building on our success with the very first such conference in Paris last year, the focus of this year's event is on a number of strategic topics concerning cyber crisis cooperation and exercises.
ENISA's International Conference on Cyber Crisis Cooperation and Exercises is becoming a unique high-profile international event that to directly supports the new cyber-security strategy of the European Union by helping various constituents in their efforts for establishing a more coherent cyber-security policy.

Additionally, the conference is a key knowledge sharing platform for national and governmental level cyber security experts.

As always, ENISA aims to facilitate debates, information exchange and offer networking opportunities to both technical experts and executive stakeholders.
Thus, this conference constitutes an essential part of the on-going, concerted EU effort to enhance network and information security and cyber crisis cooperation across Europe and beyond. So, we have a task to complete, ladies and gentlemen. Let us bear that responsibility in mind, and honour it.

As the Executive Director of ENISA, I would like to again take the opportunity to very warmly welcome all participants and wish all of you two truly inspiring and fruitful days!

Contents



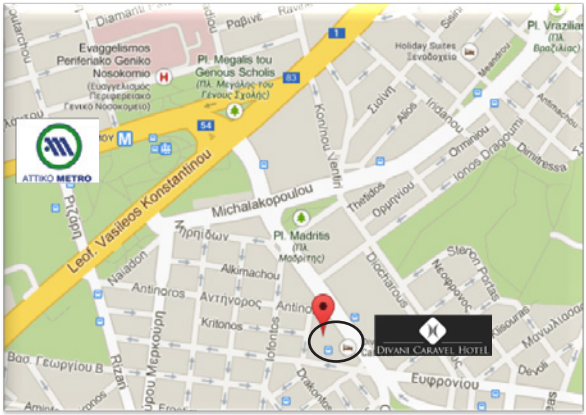
Practical Information

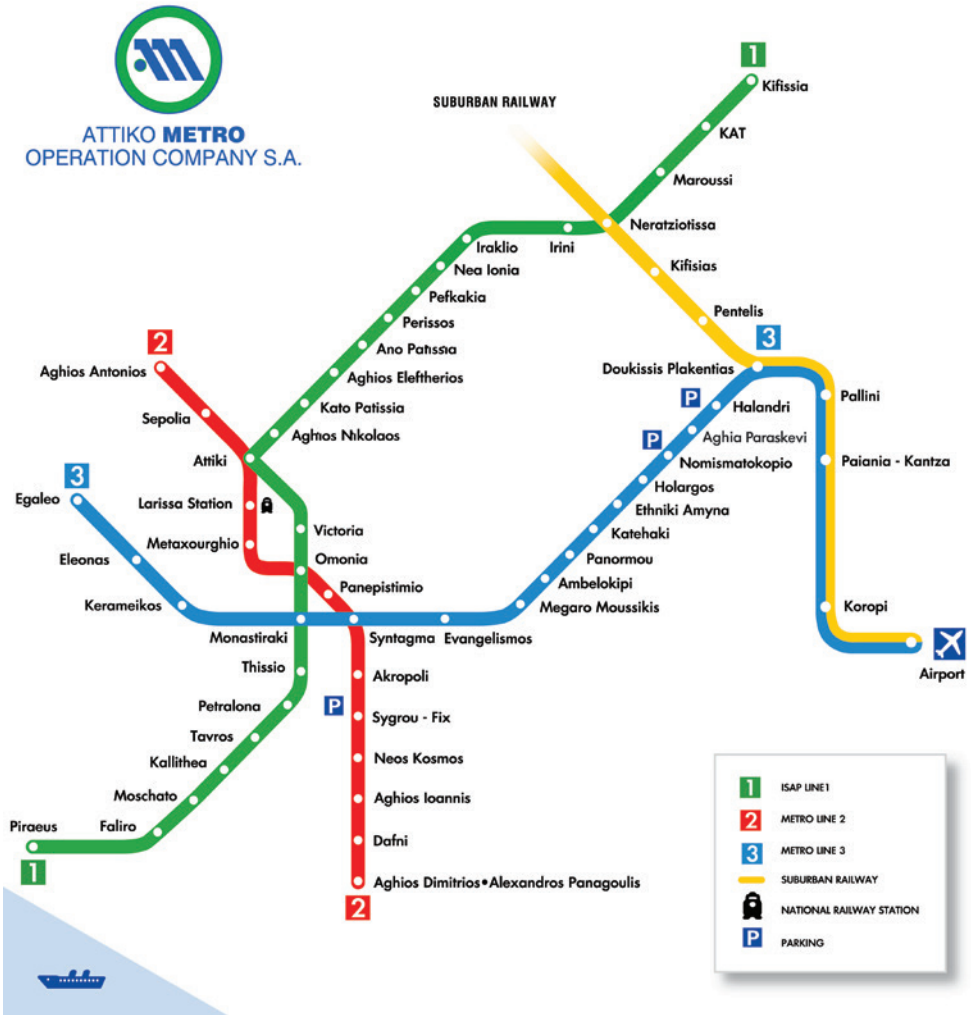
Conference Secretariat Contact Details
Mob: +306951782262
Mob: +306970015165
Email: c3e@enisa.europa.eu

Conference Venue:

DIVANI CARAVEL HOTEL

Address: Anastaseos 2, GR-15669, Papagos
Divani Caravel Hotel, 2, Vas. Alexandrou Avenue, 16121 Athens - Greece
Tel. +30 210 7207000 | Fax +30 210 7236683
Tel. +30 210 7207000 | Fax +30 210 7236683
Email: info@divanicaravel.gr
http://www.divanis.com/caravel/default-en.html




ATTIKO METRO
OPERATION COMPANY S.A.
SUBURBAN RAILWAY
1
Kifissia
KAT
Maroussi
Neratziotissa
Irini
Iraklio
Nea Ionia
Pefkakia
Perissos
Ano Patissia
Aghios Eleftherios
Kato Patissia
Aghios Nikolaos
Kifisias
Pentelis
3
Doukissis Plakentias
P
Halandri
Aghia Paraskevi
Nomismatokopio
Holargos
Ethniki Amyna
Katehaki
Panormou
Ambelokipi
Megaro Moussikis
Pallini
Paiania - Kantza
Koropi
Airport
2
Aghios Antonios
Sepolia
Attiki
3
Egaleo
Larissa Station
Metaxourghio
Eleonas
Kerameikos
Victoria
Omonia
Panepistimio
Monastiraki
Syntagma
Evangelismos
Thissio
Akropoli
P
Petralona
Sygrou - Fix
Tavros
Neos Kosmos
Kallithea
Aghios Ioannis
Moschato
Dafni
Piraeus
Faliro
1
Aghios Dimitrios
Alexandros Panagoulis
2
1 ISAP LINE1
2 METRO LINE 2
3 METRO LINE 3
SUBURBAN RAILWAY
NATIONAL RAILWAY STATION
P PARKING

Introduction

In 2012, ENISA organised the first international conference on cyber crisis cooperation. Following the success of this event, ENISA will host in September 2013 the second International Conference on **Cyber Crisis Cooperation and Exercises.**

The International Conference on Cyber Crisis Cooperation and Exercises is a unique high-profile international event that aims to directly support the new cyber-security strategy of the European Union by helping various constituents in their efforts for establishing a more coherent cyber-security policy. Additionally, the conference is a key knowledge sharing platform for national and governmental level cyber security experts. It will also facilitate debate, information exchange and will offer networking opportunities to both technical experts and executive stakeholders.

Amongst the key actions defined in the cyber-security strategy of EU that will be directly supported by **ENISA's International Conference on Cyber Crisis Cooperation and Exercises, we can mention:**

- Continuous support to the Member States and the EU institutions in carrying out regular pan-European cyber incident exercises which will also constitute the operational basis for the EU participation in international cyber incident exercises;
- Identify emerging trends and needs with regards to cyber crisis cooperation and exercises;
- Facilitate the work towards a coherent EU international cyberspace policy to increase engagement with key international partners and organisations, and to improve coordination of global cyber issues.

The conference participants will be able to further build relationships, improve trust and share good practices and capabilities on actual relevant topics like: cyber-incidents management and response co-ordination, information gathering, support platforms, tools and trusted means of information exchange and communication.

ENISA International Conference on Cyber Crisis Cooperation and Exercises is a unique opportunity to become up to date with the most relevant cyber-security trends, from a European and international perspective.

1 See also the EU Cyber-security plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive available at http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Keynote Speaker

Udo HELMBRECHT

Executive Director, ENISA

Since October 2009, Udo HELMBRECHT is the Executive Director of ENISA. Before this function, he was the President of the Federal Office for Information Security, Germany (1995 – 2003).

Also, prior to this he acted as the Director Information Processing (CIO) at Bayerische Versorgungskammer, Munich, Germany.

Udo has studied Physics, Mathematics and Computer Science, having a Diploma in Physics (Diplom-Physiker, 1981) and being also Doctor rerum naturalium (Dr. rer. nat., 1984) and Honorary Professor (2010).

Speakers

Hans Oude ALINK

NCSC, The Netherlands

Hans Oude Alink is currently the coordinator for cyber crisis management in the Netherlands. For this work he is part-time positioned in the National Cyber Security Centre in the Netherlands. Hans has a long lasting experience in the field of cyber security in several positions both at the ministry of Economic Affairs and the ministry of Security and Justice.

Ilias CHANTZOS

Symantec

Ilias Chantzos is Senior Director of Symantec's Government Relations and Public Affairs programmes for Europe, Middle East & Africa (EMEA) and Global Advisor for Critical Infrastructure and Data Protection. Chantzos represents Symantec before government bodies, national authorities and international organisations advising on public policy issues with particular regard to IT security and data risk management and availability. Prior to this role in Symantec Chantzos managed the Symantec Government Affairs Programs for EMEA and Asia Pacific Japan (APJ).

Before joining Symantec in 2004, Chantzos worked as legal and policy officer in the Directorate General Information Society of the European Commission focusing on information security policy. He covered the council of Europe Cybercrime Convention and the Framework Decision on Attacks against Information Systems. In addition, he managed a number of EU legislative initiatives relevant to information society and security, including directives on Privacy on Electronic Communications, the Data Retention Directive and the European Network and Information Security Agency (ENISA). He also represented the European Commission in various international debates and conferences.

Chantzos holds a law degree from the University of Thessaloniki and a Masters degree in Computers and Communication Law from the University of London and is a member of the Athens Bar. He serves as Chair of the Executive Board of TechAmerica Europe and appointed member of the Permanent Stakeholders Group of the European Network and Information Security Agency (ENISA) for a third consecutive term. Chantzos chaired for three terms the European policy council of the Business Software Alliance, Europe. He speaks Greek, English, Dutch and German.

Paul K. DAVIS

RAND CORPORATION

Dr. Paul Davis is a Senior Principal Researcher at RAND and a professor of policy analysis in the Pardee RAND Graduate School. He has published extensively on strategic planning, methods for such planning, decision making, deterrence, and advanced methods of analysis. Most of his applied work has been in the domain of defense planning. Earlier in his career, Dr. Davis was a senior executive in the office of the Secretary of Defense. His Bachelor's degree is from the University of Michigan and his Ph.D., in chemical physics, is from M.I.T.

Marnix DEKKER

ENISA

Dr. Marnix Dekker is NIS Expert and Information Security Officer at ENISA. Marnix works in the area of secure services and critical information infrastructures. He focuses on cloud security, smartphone security and also leads ENISA's work on the implementation of EU-wide security regulation for telco's (Article 13a). He has a Master's degree in Theoretical physics, a Ph.D. in Computer science. In his previous job he designed large national Identity Management (IdM) systems and he reviewed the deployment of a large cloud service for a critical government agency.

Freddy DEZEURE

CERT-EU

Head of CERT-EU - Freddy Dezeure graduated as Master of Science in Engineering in 1982. After joining the European Commission in 1987, he has held a variety of management functions in administrative, financial and operational areas, in particular in information technology. Since the 1st of June 2011 he leads the CERT-EU Team for the EU Institutions.

Assimoula ECONOMOPOULOU

European Centre for Disease Prevention and Control (ECDC)

Graduated from the medical school of the University of Athens in 1992, Assimoula was specialized in Clinical microbiology. After specialization, she worked for three years as medical scientific collaborator for a research programme at the school of Pharmacology of the University of Athens.
In 2003 she joined the team of KEELPNO in charge of preparations for the Athens 2004 Olympic Games, and set up a laboratory based surveillance system for the detection of foodborne and airborne diseases. From 2005-2007, she worked as a fellow of the European Programme for Intervention Epidemiology Training EPIET at the French Institute for Public Health Surveillance in Paris in Environmental epidemiology. Back to KEELPNO she was appointed head of the vector borne section. In 2011, she joined ECDC as a Seconded National Expert in the Surveillance and Response Support Unit.

Bruno HALOPEAU

European Cyber Crime Centre (EC3), Europol

Strategic & Crime Prevention Advisor in the EU CyberCrime Centre at Europol, Bruno Halopeau is also a Member of the Permanent Stakeholders' Group of the European Network & Information Security Agency (ENISA) having an advisory role to the Management Board for the Work Programme. He holds an MSc degree in Computer Science from "Ecole Supérieure d'Informatique, Electronique, Automatique" (ESIEA) in Paris and an MSc in Strategic Management & Competitive Intelligence from "Ecole de Guerre Economique" (EGE) in Paris. Being passionate about challenging engagements on Security, Safety, Business Continuity and Crisis Management issues, he gained experience with various industries including Airbus, Accenture, Sainsbury, Zurich Financial Services, ABN AMRO and KLM in implementing their CyberSecurity at various levels. He also worked for the public sector within the French Ministry of Foreign Affairs.

Kaur KASAK

NATO CCDCOE

Kaur got the first real-world experiences in cyber security when being employed as an IT security advisor by a payment agency in Estonia and as an IT specialist by Estonian Defence Forces. Last 5 years he has been working for NATO Cooperative Cyber Defence Centre of Excellence in a scientist position. My main responsibility area has been cyber defence exercises. Also, Kaur has been a project leader for organizing the following technical Blue/Red Team exercises: Baltic Cyber Shield 2010, Locked Shields 2012 and Locked Shields 2013. In addition he was the storyline leader for 4 past NATO Cyber Coalition exercises.

Amit KHOSLA

Director of Partnership Outreach and Integration Unit, National Cybersecurity and Communications Integration Center (NCCIC), U.S. Department of Homeland Security

Mr. Khosla currently serves in the Partnership Outreach and Integration Unit of the NCCIC where he is responsible for establishing information sharing relationships across public and private critical infrastructure owners and operators and leading the Cyber Unified Coordination Group for coordinated national cyber incident response. Previously serving as the Acting Deputy Director for Control Systems Security Program he gained experience in reducing industrial control system risks across critical infrastructure sectors by coordinating efforts among federal, state, local and tribal government partners, as well as industrial control systems owners, operators and vendors.

Dr. So-Jeong KIM

National Security Research Institute

EDUCATION

- Korea University, Graduate School of Information Security, Seoul, Korea
  Ph. D of Engineering(Major : Information Security Policy)
- Kyung Hee University, Graduate Institute of Peace Studies, Seoul, Korea
  Master of International Politics(Major : Northeast Asian Studies)
- Busan National University, Busan, Korea
  Bachelor of History(Major : History)
-

EXPERIENCE

Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea - Researcher of the attached institute of ETRI(NSRI), May 2004 ~ present, Senior Researcher of Policy Department

---

Klaus-Peter KOSSAKOWSKI

Trusted Introducer

Dr. Klaus-Peter Kossakowski has worked in the security field for more than 20 years. In 1988 he was one of the first members of the Virus Test Center in Hamburg where he focused on malicious network programs. He was involved with DFN-CERT – the first German CERT for an open network – a from its inception in January 1993. He successfully led the team from a research effort to a functional and well-respected operational entity in the international CERT community. Since 1998 he continues to feed back operational experiences and lessons learned to the community by being a visiting scientist within the CERT Coordination Center based at the Software Engineering Institute (SEI) working part time in several projects.

From 1998 to 1999 he was a senior consultant and project manager at secunet Security Networks AG, an German IT security provider, where he founded the internal secu-CERT team. Since 2000 he is managing PRESECURE Consulting GmbH, a privately owned company specialized in cyber security, critical information infrastructure protection, situational awareness, early warning and specialized services like CERTs or SOCs.
Kossakowski's helped considerably to raise the awareness for CERTs concentrating on international issues, cooperation, and establishing an international CSIRT infrastructure. He was elected as a member of the FIRST Steering Committee in 1997 and had been on the committee until 2005, being re-elected three times and served the two last years as Chair of the FIRST Steering Committee.

Andrea KROPACOVA

CESNET

Andrea has been working for CESNET a.l.e. since 1998. She is member of team which established first official security team of CSIRT type in the Czech Republic, the team CESNET–CERTS. The CESNET–CERTS oversees National Research and Education Network called CESNET2 provided by CESNET a. l. e. Her experience in establishing this academic team was applied in establishment of a team CSIRT.CZ, which has been officially declared by the Ministry of Interior of The Czech Republic in December 2010 as National CSIRT of the Czech Republic and has been run by CZ.NIC association since 1st January 2011. Andrea is focused on issue of network security and services, prevention and solution of security incidents and also development of provided services and security environment on national and international level.

Pierre-Dominique LANSARD

France Telecom

After a Master in Statistics from Paris, Pierre et Marie CURIE University, Pierre-Dominique joins the research centre of France Telecom where he dealt with network planning. He holds several positions in ITU for France Telecom dealing with digital networks an Intelligent networks. He then joint Global One (later Equant) where he was Head of Voice Engineering. Since 2005 he is with ORANGE (former France Telecom) Group where he heads the Critical Infrastructure Protection (CIP). Thus he is also in charge for Orange Group of the Business Continuity Management and the Crisis Management. In addition he is the Chairman of the French BCM Club.

Mariko MIYA

Cyber Defense Institute

Joined Cyber Defense Institute, Inc. in 2011. She has the expertise and knowledge of foreign and domestic cyber policies and handling cyber threats regarding national security; ranging from security concerns in the private sector to defense and critical infrastructures. In particular, her cyber intelligence reports have received high recognition from government agencies, which are written using her high-level multi-language and research capabilities. She focuses on the strategic / political side of cyber than the technical / operational side, giving practical support to sectors of the government in charge of foreign affairs and overseas information gathering and analysis, and also supports in cyber policy making.

Mats NILSSON

Eriksson

Mats Nilsson is a well known industry veteran with more than 25 years of front line experience in mobile communications. As “One of the fathers of 3G” he was deeply engaged in the evolution of mobile communications through positions as Director for Technical Strategy, Vice President for Standards and Industry Relations and lately (2009-2011) Brussels based VP and head of European affairs for Ericsson. Also piviotal in the device and aplications aspects of mobile communications thorugh being CEO of the Open Mobile Terminal Platform initiative and as Head of Ericssons Multimedia Portfolio. Now since 2011 with main focus on Cybersecurity issues and leading Ericssons engagements on all issues related to Cybersecurity, including policy, regulation, product offerings and technology leadership.

Adrien OGEE

ANSSI

Adrien Ogee works at ANSSI, the French network and information systems security agency, since 2010. His activities include international incident management and cybersecurity exercises. Before joining ANSSI, he worked for Thales in Brussels. Adrien holds a degree in information systems and telecommunication engineering from UTT and a master degree in global security from Cranfield.

Lauri PALKMETS

ENISA

Lauri Palkmets is an Expert for Computer Security and Incident Response at ENISA. Before joining the agency he was working for Estonian Defence Forces as head of Cyber Incident Response Capability. At ENISA he has been improving, extending CERT training material, and providing technical trainings for EU Member States.

Kostas PANAGOS

Corporate Security, Risk & Compliance, Vodafone

Konstantinos (Kostas) D. Panagos was born in Piraeus in 1969. He graduated from National Technical University of Athens (1994), Electronic Engineering, and holds an MBA in International Management from University of Louisville, USA. (1998).
He started his career in MICREL Medical Devices as an R&D engineer in 1993 and Quality Manager in 1994.

In 1996 he joined Panafon SA and since 1999 he served in various managerial positions. From September 2008 he holds the position of Corporate Security, Risk and Compliance Senior Manager in Vodafone Greece.
He is a member of Vodafone Group Security Leadership Team and Vodafone Group Fraud Committee.

His current interests are mainly around Security and Customer Experience, Enterprise Risk Management and Loss Prevention.
He is married and has two daughters.

Stefan RITTER

BSI, Germany

Since 2007, Stefan Ritter is head of CERT-Bund and the national IT-situation centre at the German Federal Office for Information Security BSI at Bonn. The years before he collected exercise experience as a senior expert for critical information infrastructure protection and as an officer at the German armed forces. Since 2009, his team provides dedicated cyber exercise support. Together they supported the preparation and played most of the large national and European cyber exercises.

Wolfgang ROEHRIG

European Defence Agency

Wolfgang Röhrig was born 14 February 1966 in Troisdorf-Sieglar, Germany and entered the German Navy as officers candidate in 1985. After completing his studies at the University of the Federal Armed Forces in Hamburg with the degree of a MBA he served in several officer positions in the German Navy and the German Joint Services including several operational deployments and service in NATO. Since the mid of the 1990 he specialized on communications and information systems. Since March 2012 he is appointed as Project Officer Cyber Defence at European Defence Agency (EDA). Wolfgang Röhrig is married to Aneta Röhrig and they have two children.

Luigi ROMANO

University of Naples Parthenope

Luigi Romano is currently a Full Professor at the University of Naples “Parthenope”. His research interests are networked computer system security and dependability, with focus on Critical Infrastructure Protection (CIP). He is the Chair of the Cyber Security technology area within the context of the SERIT (Security Research in ITaly) initiative. SERIT is the technological platform for national security jointly promoted by the National Research Council (CNR) and Finmeccanica.

Ann-Sofie RONNLUND

DG CNECT

Ann-Sofie Ronnlund is a Policy Officer in the Trust & Security Unit of DG Communications Networks, Content & Technology (CNECT) of the European Commission and has been involved throughout the process leading up to the adoption of the Cybersecurity Strategy of the EU, the accompanying legislative proposal on network and information security and the preceding impact assessment. She also has experience from working in the European Parliament and in the technology sector before joining the European Commission in 2005.

Adam SEDGEWICK

NIST, US

Adam Sedgewick serves as Senior Information Technology Policy Advisor at the National Institute of Standards and Technology. In this role, Sedgewick represents NIST on the Department of Commerce Internet Policy Task Force and advises NIST leadership on cyber-security issues. Previously, Adam was Senior Advisor to the Federal Chief Information Officer Council, coordinating cross-agency initiatives and assisting in the implementation of policy and directives. Sedgewick is also leading NIST's project to develop a cybersecurity framework for critical infrastructure sectors, as called for in President Obama's Executive Order on "Improving Critical Infrastructure Cybersecurity."
Adam served as Professional Staff Member for the Senate Committee on Homeland Security and Governmental Affairs for nine years, handling cyber security and federal information technology policy.

Omar SHERIN

Q-CERT

Omar Holds a Bachelor of Science degree in computer engineering with more than 10 years of professional Information security, resiliency experience. Omar is a member of the OWASP foundation leader's board and a voting member in the IEC/ISA-62443 standard for critical infrastructures resiliency and an international partner in the Industrial Control Systems Joint Working Group (ICSJWC) created by the DHS. He has worked for several multinational firms in the oil and gas sector, Omar is a certified CBCP, CRISC, CEH and ISO27001LA and in his spare time an active blogger in (ciip.wordpress.com) and a regular speaker on information security and CIIP issues, currently he is the ictQATAR/QCERT Head of CIIP participating in assessing the critical infrastructures and in drafting national cyber security laws, standards and guidelines like the National ICS security standard, the Qatari government cloud security policy, and the government mobile devices security guidelines.

Zarko SIVCEV

EUROCONTROL

Žarko Sivčevis currently Advisor to the Director in EUROCONTROL's Network Manager Directorate. He got a degree in Air Traffic and Transport Engineering from the University of Belgrade. In 1986 Žarko joined Operations Department of Adria Airways in Ljubljana, Slovenia. In 1992 he moved to Brussels where he participated in the development and operational implementation of EUROCONTROL's Central Flow Management Unit. In 2010 Žarko was a member of the EUROCONTROL volcanic ash crisis team. Later on he participated in the development of the European Aviation Crisis Coordination Cell (EACCC), a body established to coordinate management of response to the network crisis affecting aviation in Europe. At present Žarko Sivčev is Operations Manager of the EACCC.

Jason THELEN

Brent Scowcroft Center on International Security

Jason Thelen is the associate director of the Cyber Statecraft Initiative of the Brent Scowcroft Center on International Security. He leads the Atlantic Council's programming on cybersecurity, focusing on cybercrime, cyberespionage, and cyberwarfare.

Mr. Thelen earned his law degree from the Washington College of Law at American University, where as a legal fellow, he focused on issues of national security, habeas corpus litigation, federal jurisdiction, separation of powers, the law of armed conflict, and executive privilege. He also served as an editorial board member for the American University International Law Review and was a founding executive board member of the American University Business Law Review. During law school, Mr. Thelen studied abroad in Paris, Brussels, Geneva, and London, where his coursework concentrated on human rights and international economic law at the European Union, the World Trade Organization, International Committee of the Red Cross, and the United Nations.

Concurrent with law school, Mr. Thelen completed a master's degree in international affairs from the School of International Service at American University, where his studies focused on international politics and defense policy. Prior to attending American University, Mr. Thelen began his career in the private sector working in the institutional investment management industry during the 2008 global financial crisis.

Mr. Thelen, a native of Eugene, Oregon, received his BS from Southern Oregon University and is a member of the Oregon State Bar.

Panagiotis TRIMINTZIOS

ENISA

Dr Panagiotis TRIMINTZIOS is managing the area of Cyber Crisis Cooperation and Exercises within the Information Security and Data Protection Unit at the European Network and Information Security Agency (ENISA), where he works since 2005. He was the director of Cyber Europe 2010, the first pan European large scale cyber exercise, Cyber Atlantic 2011, the first EU-US cyber exercise, Cyber Europe 2012, the second pan European exercise with over 500 participants. His other projects in the area of cyber crisis cooperation and management include studies on National Cyber Contingency Plans, National Risk Assessment, pan European Cooperation Operational Procedures etc. In the past he managed studies on Resilience Metrics, Resilience of the Internet Interconnection Ecosystem (Inter-X). For many years he was the Editor-in-Chief of ENISA's Quarterly Review. Dr TRIMINTZIOS holds a BSc on Computer Science, an MSc on Computer Networks and Telecommunications, a PhD on IP Networks Management, while prior ENISA for many years worked as a researcher managing European and nationally funded projects in his areas of expertise. He has published over 60 papers in scientific journals, magazines, and international conferences.

Claire VISHIK

Intel

Claire Vishik's work at Intel Corporation UK focuses on hardware security, Trusted Computing, privacy enhancing technologies, some aspects of encryption and related policy issues. Claire is a member of the Permanent Stakeholders Group of ENISA, the European Network and Information Security Agency, Council member for the Information Security Forum, and a member of numerous other advisory and review boards in several areas of security and privacy. She is active in standards development and R&D strategy and is on the Board of Directors of TCG, the Trusted Computing Group and Cybersecurity Research Alliance. Claire received her PhD from the University of Texas at Austin. Prior to joining Intel, Claire worked at Schlumberger Laboratory for Computer Science and AT&T Laboratories, focusing on security and other aspects of Internet and computing technologies, from electronic commerce and communication protocols to software systems and applications. Claire is the author of many papers and reports and 30 pending and granted US patents.

Pieter WELLENS

DIGIT

Pieter Wellens (1962) started his professional career in the Belgian Army (1987) as Officer Engineer in the telecommunication troops. After 10 years of experience in military telecommunications, he joined the Belgian General Police Support Service as IT expert where he was responsible for the integration of international police communication systems (EUROPOL, Schengen and Interpol) and the implementation of information systems in support of the Belgian police services. Since 2000 he is dealing with trans-European communications as an EU civil servant for the EC/ DG DIGIT. Today Pieter is head of sector responsible for Trans-European and External Networking Services (TENS)

Agenda - Day 1

23 September 2013

Timing	Theme
08:30 -09:00	**Registration**
09:00 -09:40	Welcome & introduction **Keynote: Prof. Udo HELMBRECHT, Executive Director, ENISA**
09:40-11:00	**Session:** Governance models, practices and cooperation procedures for cyber crisis management **Speaker 1:** Adrien OGEE. ANSSI, France – Multilateral mechanisms for cyber crisis cooperation in the EU **Speaker 2:** Adam SEDGEWICK, NIST, US – The Development of the Cybersecurity Framework for Critical Infrastructure in the United States **Speaker 3:** Ann-SOPHIE, European Commission – The European Cybersecurity Strategy and draft Directive on Network and Information Security: Enhancing cybersecurity capabilities and cooperation throughout the EU **Speaker 4:** Hans Oude ALINK NCSC, The Netherlands - Public Private partnership in Cyber crisis in the Netherlands: The ICT Response Board Chair: Iowa CARELS, National Cyber Security Centre, The Netherlands
11:00-11:30	**Coffee break**
11:30-13:00	**Session:** Cyber crisis management and cooperation exercises **Speaker 1:** Stefan RITTER, BSI, Germany - How 'Jigsaw' exercises can increase effects of information sharing during cyber-exercises **Speaker 2:** Amit KHOSLA, DHS, US, The US National-Level Exercise 2012 – setup and main lessons learned **Speaker 3:** Freddy DEZEURE, CERT-EU - APT response; shared threat intelligence to detect early and respond quickly **Speaker 4:** Roger HOLFELDT, MSB, Sweden - The National Cyber Exercise in Sweden **Chair:** Rob HARRIS, Cyber Security Operations Centre (CSOC), UK
13:00-14:00	**Lunch break**

Timing	Theme
14:00-15:15	**Session:** Governance models, practices and cooperation procedures for general crisis management **Speaker 1:** Zarko SIVCEV, EUROCONTROL - Aviation Crisis Management in Europe - Lessons Learned from the First Cyber Attack Exercise - CYBER 13 **Speaker 2:** Assimoula ECONOMOPOULOU, European Centre for Disease Prevention and Control (ECDC) – Information Processing for Public Health **Threats:** an EU perspective **Speaker 3:** Bruno HALOPEAU, European Cyber Crime Centre (EC3), Europol – Practices and cooperation related to Cybercrime **Chair:** Helena RAUD, National Information Systems, Estonia
15:15-15:45	**Coffee break**
15:45-17:30	**Session:** Cyber-exercise scenarios: supply chain integrity **Speaker 1:** Pierre-Dominique LANSARD, France Telecom - Scenarios/case studies on Supply Chain Integrity **Speaker 2:** Luigi ROMANO, University of Naples Parthenope - The Big Challenge: Building Trust while favouring Openness **Speaker 3:** Claire VISHIK, Intel - Towards a standard approach to supply chain **Speaker 4:** Mats NILSSON, Eriksson - Supply Chain Integrity and Security Assurance for ICT - Finding practical approaches to ensure security in a fast evolving and all-embracing mass market **Speaker 5:** Kostas PANAGOS Corporate Security, Risk & Compliance, Vodafone - A trusted supplier counts Chair: Demosthenes IKONOMOU, ENISA
17:30	Day 1 Closed
20:00	**Social Event (by invitation only)**

Summary of presentations

Day 1

Hans Oude ALINK

Public Private partnership in Cyber crisis in the Netherlands: The ICT Response Board

This presentation will focus on the way in which in the Netherlands the important stakeholders (both public and private) can contribute during an cyber related crisis situation. For this purpose a formal advisory board has been implemented in which these stakeholders work closely together during a cyber crisis. The goal of the board, called the ICT Response Board (IRB), is to give the decision makers in the Netherlands a expert advise how to deal with the specific crisis situation. The IRB has proved its relevance during some crisis situations since its existence in 2011.
The IRB proves to be beneficial for both public and private partners. The trusted information sharing within the Board provides both parties with more information then they usually would receive during such crisis. Private partners help shaping the decision-making process in which their interests are properly covered. Public partners receive the information that really matter for the handling of the crisis in a timely way.

Freddy DEZEURE - CERT-EU

APT response; shared threat intelligence to detect early and respond quickly

Targeted attacks are becoming ever more important threat for businesses and public services alike. These attacks also become ever more sophisticated with malware and C&C infrastructure made to measure. Infection is difficult to avoid and therefor early detection and fast remediation are key to the response. The presentation will present lessons learnt in real life cases, illustrating the value of intelligence sharing collaborationships with private industry and national CERTs as well as the usefulness of information sharing platforms and information exchange standards.

Assimoula ECONOMOPOULOU - European Centre for Disease Prevention and Control (ECDC)

Information processing for public health threats, from an EU perspective

ECDC is an EU agency. Its mandate is to identify, assess and communicate on public health threats (PHT) due to infectious diseases. Early Warning and Response System (EWRS) and Epidemic Intelligence Information System (EPIS) are two systems developed in order to gather information on PHT in a timely manner. The EWRS is an official web based system linking the Commission to Member States (MS) and ECDC, while the EPIS is an web based, unofficial platform, where information are shared among experts of MS. To assess PHT, in a daily base, Epidemic Intelligence officers at ECDC are proceeding to the analysis of signals coming from different official sources such as EWRS, EPIS as well as from International organisations, and non EU countries public health institutions. They also consult web unofficial information sources. Threats detected are reported to the European Commission daily. Risk assessments are undertaken when needed according to established criteria and they are published to the website.

Bruno HALOPEAU - European Cyber Crime Centre (EC3), Europol

Practices and cooperation with Law Enforcements and CERTs for Operational and Crisis purposes

With so much of our everyday communication and commercial activity now taking place via the Internet, the threat from cybercrime is increasing, targeting citizens, businesses and governments at a rapidly growing rate. The EU in particular is a key target because of its advanced Internet infrastructure and increasingly Internet-based economies and payment systems.
Today, EC3 has been set-up to tackle the issue of CyberCrime and the centre has to be an efficient coordination centre not only for on-going operations but should also be ready to respond or support Member States in crisis situations by providing expertise, ready-to use platforms and facilities, and facilitating communications between trusted actors

---

Amit KOSHLA

Overview of the US National-Level Exercise 2012

Mr Koshla will provide an overview of the National-level Exercise (NLE) 2012, which focused among others on cyber. This exercise substituted the Cyber Storm series in 2012. The presentation will provide the overview, the set up and the lessons learned from the exercise.

Pierre-Dominique LANSARD

Telecom scenarios to insure supply chain integrity

This paper will address scenarios for supply chain integrity within a telecom operator.
The most important supply is the power supply and this is the one which is, by far, the more absorbing. Not only we have to be sure that on a day to day basis the Power supply operator will deliver smoothly but in case of power outage we have to be sure that the fuel supplier will also deliver on require to fill up the generators.
The second highest power supply is the human resource. In a lot of circumstances one could have the best plans of the world if the right person is not available at the right time at the right place then you process is 99% out of order. This is all about business continuity.
Another concern is about so called "old technology" spare parts like for instance in the circuit switch network where it becomes more and more difficult to find spare parts and nevertheless important official governmental private networks remain under such a technology.
There is also a need obviously to maintain the accounting chain.

Mats NILSSON – Eriksson

Supply Chain Integrity and Security Assurance for ICT - Finding practical approaches to ensure security in a fast evolving and all embrcing mass market

The ICT sector is rapidly evolving as an all embracing mass market - The networked society. It is a global market with global supply chains of software and hardware, forming a global ecosystem of various roles and components. Thus the end products will have components from your own development, sourced proprietary software and hardware, elements from open source communities, open runtime invironments and app/content stores etc..

Then on top of that you have integration and operation of such products as nessesary elements producing the end service. There are several functional, technology and process elements that are effective in the context of sensuring supply chain integrity. However means to ensure supply chain integrity, like any form of security assurance, needs to be based in a pragmatic risk analysis and cost benefit performance analysis. Different public and private actors have ther respective roles in ensuring supply chain integrity, standards, best practises and collaborateive actions through CERTs and incident report handling mechanisms are important tools in this respect. The presentation will discuss how to effectively use such tools as a pragmatic way to resolve supply chain integrity issues.

Adrien OGEE – ANSSI

Multilateral mechanisms for cyber crisis cooperation

The EU Standard Operating Procedures (SOPs) have been developed by European cybersecurity crisis managers over the 2010-2013 period, with one objective in mind: to improve operational level information exchange and cooperation between EU Member States during multinational cybersecurity crises, in order to fasten the understanding of their causes and the mitigation of their impacts. The SOPs have been put to the test on several instances and proved that, following simple rules, international cooperation activities during cyber crises could help to define crisis exit scenarios.
Such mechanisms could be easily adapted to different contexts, such as regional or public-private cooperation. The presentation will cover the core mechanisms of the SOPs and touch upon the European Cyber Crisis Cooperation Framework (ECCCF), the overall framework developed by Member States and which the SOPs are part of.

Stefan RITTER - BSI

More fun with exercises! - Multilevel Clustered Exercise Framework

Multinational exercises create a lot of experience and lessons learned within organizations. But they hardly reach their objective to initiate real information sharing and multinational collaboration between participating nations. This presentation shows first results of a BSI concept for a „Multilevel Clustered Exercise Framework". To make information sharing exercising more fun, the idea is to create a scenario of multiple jigsaw pieces that must be collected and brought together. And there could be "keys" (like passwords), that others discover and need to be transferred to the "locks" (encrypted file or malware) to unlocked your treasure chest (new information, C&C, …). By design, the crisis-situation can only be solved by cooperation and sharing. And "working and sweating together" forms teams. Some structural helping ideas will be presented as of course preparation is more laborious for scenario stories and elements like this.

Holfeldt ROGER

NISÖ 2012

NISO 2012 was the largest cyber exercise conducted in Sweden where society's ability to manage It-related crises were put into focus. The exercise was organized by MSB and involved a number of government agencies and private operators at the national level. NISO 2012 also included a Nordic participation from National CERT-functions.
The scenario focused on cyber security and vital societal functions in the sectors of energy, telecommunications and transport were exposed to strain. In practice, the operators managing a serious it-related crisis were in a context, which demanded rapid coordination to take relevant action, to be successful in managing the crisis.
The exercise contributes to develop capacity for cooperation and coordination between private and public actors in the management of such an event. Regular national exercises are essential to develop and evaluate structures for the management of serious It-related crises. Experiences of past cyber incidents and It-related crises shows that it is important to have an organization that is prepared.

The presentation will cover details on how the exercise was arranged and conducted. It will also touch upon lessons identified and areas for development.

Luigi ROMANO

The Big Challenge: Building Trust while favouring Openness

The objectives of this talk are: 1) To present a (purposely) un-balanced analysis of pros and cons of the Open Source and Closed Source software development models (and related Supply Chain), 2) To provide evidence that there is a strong business case for Open Source Software (OSS) adoption, and thus an equally strong motivation for chasing Supply Chain Integrity (SCI) trust models that are rigorous, while still favour openness, 3) To stimulate discussion, in an attempt to define a strategy for effective research, to be done jointly by industry and academia, towards the development of such improved trust models, and 4) To make proposals for immediate action points to extend the network of experimenters willing to participate in the ENISA Cyber Exercises upcoming campaign on SCI integrity. The analysis is done with respect to three recommendations from the ENISA study on SCI, namely: Recommendation 1 (Improved and innovative trust models), Recommendation 3 (Deeper study of good practices), and Recommendation 7 (Opportunity for industry and academia to study balanced approaches).

Ann-Sofie RONNLUND

The European Cybersecurity Strategy and draft Directive on Network and Information Security: Enhancing cybersecurity capabilities and cooperation throughout the EU

Preparedness and cooperation against cybersecurity risks and incidents has a crucial role to play in delivering a safer on-line environment, in the EU and beyond. Cyber incident exercises are an important tool for testing and enhancing capabilities. The EU Cybersecurity Strategy puts emphasis on pan-European cyber incident exercises and the draft NIS Directive would require all Member States to have NIS cooperation plans in place and regularly test them through exercises. It also foresees a NIS cooperation plan for the EU. Preparedness would be further strengthened through appropriate risk management measures, as laid down in the draft NIS Directive. In order to help implement the measures set out in the NIS Directive and ensure its convergent and harmonised application across the EU the European Commission has launched a public-private NIS platform, which gathers a broad range of industries, with the aim of identifying and facilitating the up-take of risk management and information sharing best practices and identifying future research and technological needs.

Adam SEDGEWICK - NIST, US

The Development of the Cybersecurity Framework for Critical Infrastructure in US

In February 2013, President Barack Obama issued the Executive Order "Improving Critical Infrastructure Cybersecurity" directing the National Institute of Standards and Technology (NIST) – a technical agency within the US Department of Commerce – to develop a voluntary framework for reducing cybersecurity risks to critical infrastructure. The Framework will consist of standards, guidelines, and best practices. The Framework is intended to help businesses manage cybersecurity risk while maintaining flexibility and the ability to meet evolving business needs.

The Framework is also been designed to allow for the use of industry-developed standards that can scale internationally. As many organizations operate globally or rely on the interconnectedness of the global digital infrastructure, diverse and unique requirements can impede interoperability, hinder innovation, and ultimately harm cybersecurity needs. A discussion draft of the Framework was shared on August 28, 2013, containing initial considerations, and a preliminary draft will be published in October.

Zarko SIVCEV

Aviation Crisis Management in Europe - Lessons Learned from the First Cyber Attack Exercise - CYBER 13

The eruption of the volcano Eyjafjallajökull in Iceland in April and May 2010 demonstrated the vulnerability of the European aviation system and required urgent action. Using lessons learned, Europe, led by European Commission (EC) and EUROCONTROL, established the European Aviation Crisis Coordination Cell (EACCC) on 19th May 2010. The main role of the EACCC is to support coordination of the response to network crises impacting adversely on aviation, in close cooperation with corresponding structures in States.

To ensure an improved level of preparedness in Europe for any kind of crisis situations EACCC has been involved in regular exercises. On 29-30 May 2013 the EACCC organised its first cyber attack exercise, CYBER 13, which simulated the outage of the NM communication lines and its impact on the NM services together with the continuous outage of communications lines in participating States, causing major disruption to the European air traffic. The participants included representatives from France, Germany, Italy, Poland, The Netherlands, The United Kingdom, Maastricht Upper Area Control Centre (MUAC), Air France, Brussels Airlines, Flybe and Lufthansa and members of the EACCC and observers from various services from the European institutions dealing with crisis management and/or cyber security, including ENISA.

Claire VISHIK

Towards a standard approach to supply chain

In today's global economy, almost all technology products depend on global supply chains. As the dependence on ICT technologies increases in all areas of life and work, concerns have been expressed about the integrity of diverse international supply chains. Standards bodies, from NIST to JTC1, responded to these concerns by developing standards addressing various aspects of supply chain integrity. Organizations in various industry segments developed best practices to deal with international suppliers and global supply chains. On the procurement side, governments and industry developed best practices.

The field of supply chain integrity has accumulated a lot of useful information that is usually adapted to specific contexts of use. These approaches work well in areas that they serve, but the need for a coordinated general framework that unifies these ideas is felt by technologists working in this area and is reflected in emerging efforts in standards bodies and industry associations.

This talk reflects the results of work of ENISA's expert group on supply chain integrity and subsequent developments in this area.

Pieter WELLENS – DIGIT

Testa new generation

TESTA (Trans European Services for Telematics between Administrations) is a communication platform to exchange electronic data between European and Member States administrations in a secure, reliable and efficient way.

Mission: to facilitate cooperation between public administrations in various policy areas, and to consolidate existing networks by providing a secure, reliable and flexible communication service layer.

Agenda - Day 2

24 September 2013

Timing	Theme
08:45-09:00	**Registration**
09:00-10:00	Opening speeches: **Speaker 1:** Ilias CHANTZOS, Symantec - The trends of cyber incidents leading to large-scale cyber-crises **Speaker 2**: Jason THELEN, Atlantic Council US - Global Aggregation of Cyber Risk: 'Finding Cyber Sub-Prime' **Chair:** Panagiotis TRIMINTZIOS, ENISA
10:00-11:00	**Session:** Issues Cyber Security Crisis Cooperation, Management and Information Exchange **Speaker 1:** Mariko MIYA, Cyber Defence Institute, Japan, Major Cyber Incidents in Japan **Speaker 2:** Marnix DEKKER, ENISA – European Network and Information Security Incidents Report 2012 **Speaker 3:** Dr. So-Jeong KIM, National Security Research Institute, S. Korea - Cyber-security in the Republic of South Korea **Chair:** Paul RHEIN, Haut-Commissariat à la Protection Nationale, Luxemburg
11:00-11:30	**Coffee break**
11:30-13:00	**Session:** Technical Issues on Cyber Crisis Cooperation and Exercises **Speaker 1:** Kaur KASAK, NATO CCDCOE - Lessons learned from the Locked Shields 2013 exercise **Speaker 2:** Lauri PALKMETS, ENISA - Technical trainings for CERTs **Speaker 3:** Omar SHERIN, Q-CERT, Qatar - 2013 CS drills for the Energy sector in Qatar **Speaker 4:** Andrea KROPACOVA, CESNET - DDoS attacks against www server providers in the Czech Republic **Chair:** Andrea DUFKOVA, ENISA
13:00-14:00	**Lunch break**

Timing	Theme
14:00-15:00	**Session:** Infrastructures related to Cyber Crisis Cooperation and Exercises **Speaker 1:** Wolfgang ROEHRIG, European Defence Agency (EDA) - Mainstreaming European Military Cyber Defence Training & Exercises **Speaker 2:** Pieter WELLENS, DIGIT - The sTesta infrastructure **Speaker 3:** Klaus-Peter KOSSAKOWSKI, Trusted Introducer, Operational Support Services for Cyber Response Teams in Europe and beyond **Chair:** Razvan GAVRILA, ENISA
15:00-15:30	**Coffee break**
15:30-17:15	**Panel Session:** Challenges and approaches of Cyber Risk Assessments **Speaker 1:** Panagiotis TRIMINTZIOS, ENISA - ENISA's Guide on National Risk Assessment for ICT **Speaker 2:** Amit KHOSLA, DHS, USA– Approaches in National Cyber Risk Assessments **Speaker 3:** Costas EFTHYMIOU, OCECPR, Cyprus – The Cyprus efforts in NRA and National Contingency Plans **Chair:** Neil ROBINSON, RAND Europe
17:15-17:30	Closing remarks

Summary of presentations

Day 2

Ilias CHANTZOS

The trends of cyber-incidents leading to a cyber-crisis. From large scale attacks to large scale targeting

Mr. Chantzos will compare large scale cyber attacks and the modus operandi in the past with recent attack practices. He will then give examples of how organized groups successfully target and compromise a large number of organizations through concerted persistent and targeted attacks over a significant period of time. He will highlight some of the defense strategies that are needed against this constantly evolving threat.

Marnix DEKKER

Cyber Incident Reporting in the EU

Summary: Incident reporting (after the incident was resolved) helps us understand threats, vulnerabilities and the impact of incidents. Incident reporting is vital to improve risk assessment, and to allow industry and government to improve cyber security. The 2009 reform of the EU legislation for e-communications obliges providers of e-communications to report cyber incidents to national regulators. Regulators in turn provide a summary of significant incidents to ENISA and the EC. This step allows ENISA to aggregate data and provide an annual EU wide report. It also allows us to start discussions and address specific types of incidents, working together with government and industry experts. The recently proposed cyber security directive contains similar provisions, this time covering also other sectors. This directive aims to cover critical infrastructure, including for example cloud services and payment gateways. Marnix will give an overview of the different types of incident reporting legislation in the EU and discuss how to set up an efficient and effective framework of incident reporting across Europe.

Costas EFTHYMIOU

First steps towards a national cyber risk assessment

A comprehensive risk assessment in the area of cybersecurity, on the national level, is vital for the effective mitigation of cyber threats that can have national impact. Cyprus is a small country but faces many of the same challenges that larger countries do in this field. We plan to conduct a national risk assessment in the coming months based on the interdependencies between critical infrastructures (CIs), and the relevant working group is comprised of a number of stakeholders that are absolutely necessary to conduct this analysis with effective results and full use of limited resources. The type of approach to be used (decentralised/centralised and service/asset/impact based) will be discussed within the group and tailored both to the nature of our CIs and the size of the country. We consider that this approach will aid the correct identification of all critical information infrastructures (CIIs) that need to be taken into account, create a solid basis for the development of a National Contingency Plan for CIIs and that the results of the national cyber risk assessment will provide valuable input to a number of actions that have been identified and that will be carried out under the National Cybersecurity Strategy.

Kaur KASAK - NATO CCDCOE

Locked Shields 2013 exercise and lessons for the future

In this talk we give a brief overview of technical cyber defence exercise (CDX) Locked Shields 2013 which was organized by NATO CCD COE jointly with several partners. We describe the setup, attack campaign and observed defensive methods and tactics. Key lessons will be pointed out focusing on how to improve future exercises.

We have experience in executing Blue/Red Team CDX on 3 technical platforms. All of them have had different architecture, underlying virtualization software, management tools and so on. This makes sharing the content and technical solutions difficult. As a lot of nations and organizations have their own cyber ranges it would be beneficial to increase collaboration and unify the platforms. We would like to map the interest of conference participants to share the building blocks of cyber ranges and to contribute into the creation of common platform which could be used for executing large-scale international exercises.

So Jeong KIM

Cyber Security of ROK

Cyber security gets more attention these days in ROK. With the geopolitical reason, well advanced IT system of S. Korea has suffered many cyber incidents since 2003. In this year particular, we had 3.20 cyber attack and 6.25 cyber attack. Those are different from what we've suffered in technically. They were the APT attack. Again some attacks were originated from N. Korea for political reason by media just like 2011 DDoS attacks.
I will introduce how many accidents were occurred in S. Korea and how well we responded those incidents and then I will look into the cyber security system of ROK such as governance, legislations, etc. The Blue House controlled the cyber security and gets assistance from various government agencies, for example, intelligent agency, ICT agency and military department for various sectors of privacy protection, infrastructure protection, cyber crime prevention and detection. Also, I will briefly explain the 2013 Seoul Cyberspace Conference in October. The Seoul Conference deals with 6 agenda including cyber security and international security.

Andrea KROPACOVA - CESNET

(D)DoS attacks targeted web servers operated in The Czech Republic

At the beginning of March 2013, web services that are provided in the Czech Republic became the target of a series of (D)DoS attacks. Attacks targeted a different group of servers each day – web servers of the most popular news' media on Monday, the most widely used search engine seznam.cz on Tuesday, web servers of several banks on Wednesday and web servers of two mobile operators on Thursday. The series of attacks were well prepared – by means of planning, selection of the targets, good order of the targets, volume of the attacks and methods used for attacks. This situation was very enlightening for the Czech Republic and its internet community.
The presentation describes the details about the type of the attack, what type of solution and defence mechanisms were used to eliminate the attacks, process of information sharing and assessment and the role and actions of existing Czech CERT/CSIRT teams during the attacks at national and international levels. The presentation will also inform about positive and also negative outcomes (lessons learned) from this situation, observations and changes started by this event in the Czech Republic.

Mariko MIYA

Findings from Massive Cyber Attacks in Far East Asia Region

Every year, there are massive cyber attacks from China to Japan around September 18. This day is the day of the 918 Incident (otherwise known as Manchurian Incident or Mukden Incident), which is a military conflict / political incident which took place in northeast China on September 18, 1931.
There have been reoccurring cyber attacks every year around this day, and Cyber Defense Institute has monitored and analyzed the incident through the years, and have found a certain pattern in the mechanisms in which these massive cyber attacks emerge. In the example of 2012, there were few hundred cases of website defacement and DDoS attacks which started from around 9/12 which increased day by day until the X-Day, 9/18.
This speech will be about our findings and lessons learned, where I expect to be able to talk about this year's event yet to come (during 2013/9/10-9/18), as well as the March 20th cyber attack that happened in South Korea this year, and other massive cyber attack incidents that have been happening in Far East Asia.

Lauri PALKMETS

Technical trainings for CERTs

ENISA CERT training presentation will give an overview on how the initial exercises program has evolved into full scale training portfolio, and brings insight on how is the material created. Additionally the presenter will give you an overview how the material could be useful for your organisation.
The initial target audience of the trainings has been Cyber Emergency Response Teams, but the material could be efficiently used by everyone interested.
ENISA CERT training and exercise material was introduced in 2008, in 2012 it was complemented with new scenarios containing essential material for success in the CERT community and in the field of information security. The new the material, created in 2013, touches the area of Cyber-Crime, and provides new insight in practicing on how to cooperate with Law Enforcement Agencies. On this page you will find ENISA CERT training and exercise material, containing Handbook for teachers, Toolset for students and Virtual Images to support hands on training sessions.

Wolfgang ROEHRIG - European Defence Agency

Mainstreaming European Military Cyber Defence Training & Exercises

With reference to European Defence, it is assumed that in the next 5-10 years skilled and competent Cyber Defence personnel will be a scarce and expensive resource.
The Defence part of the EU Cyber Security strategy emphasizes on awareness, skills and training. The EU, integrating civil and military responsibilities for Europe, is the ideal ground to plant and grow the development of a common Cyber Security/Defence culture and understanding especially allowing close cooperation with the civil cyber security community. This unique characteristic of EU is the necessary setup for synergies and innovative solutions.
The European Defence Agency recently concluded a holistic landscaping study on Cyber Defence capabilities, taking into account what exists in member states and EU institutions both on the civil and the military side. This study gave EDA the impulse to pursue several work strands, including Cyber Defence Training and Awareness to improve Cyber resilience of future CSDP operations. In close cooperation with the Member States and EU institutions EDA has taken several education, training and exercise related work strands on its agenda in order to ease the pressing skills, competency and awareness problem. Beside conducting a structured Cyber Defence Training Need Analysis, EDA has initiated a specific activity targeting to support training and exercises with appropriate IT infrastructure; the so called Cyber Ranges project.
The EDA presentation will address training related findings of the stocktaking study and the current EDA activities on training, exercises and awareness

Jason THELEN, Atlantic Council US

Global Aggregation of Cyber Risk: "Finding Cyber Sub-Prime"

Responding to real impacts on financial performance from cyber incidents, requires important business trade-offs that dramatically "raise the stakes" for getting cyber-security right. Leading board directors and executives are much more closely integrating business needs and imperatives with cybersecurity decision-making and risk management. Meanwhile, today's cyber trends echo those of the 2008 financial crisis, where risks were securitized, chopping them up and selling them off in ways that few if any could understand. The resulting crash affected everyone, even those who were not directly exposed to the underlying risky securities. Similarly, strong cybersecurity may not shield even the best-protected companies from cascading cyber shocks. Decision-makers who recognize unidentified or misidentified risks can better protect against threats to the health of the system. This presentation examines the results of year-long study on interrelated cyber hazards and underlying risks. The study considers the role of the insurance industry, along with lawmakers, regulators, and corporate executives and directors, to lead the way to responsible risk management.

Panagiotis TRIMINTZIOS - ENISA

Study on National-level Cyber Risk Assessments

ENISA is currently undertaking research on national-level risk assessment and threat modelling methodologies used for (critical) ICT infrastructures. National risk assessments and modelling are essential processes in the context of developing and updating National Network and Information Security (NIS) cooperation/contingency plans, which in turn is one of the pillars within a National Cybersecurity Strategies. The talk will present objectives in this study in identifying the valuable approaches, practices and challenges that countries have experienced on assessing risks of (critical) ICTs infrastructures, the dependencies and the challenges. The results of the analysis would be used by ENISA to help all countries in Europe to learn from the experiences and practices of others, hoping to close the maturity gap.

Additional Guidance

Hotels

The following rates can be used for the purpose of ENISA Conference.

Hotel Name	Address	Phone number	Room rate Single	Room Rate Double Occu-pancy	High Speed Internet Access Included	Ref code
Hotel Di-vani-Caravel*	2 Vas. Alexandrou Ave	30 210 7207000	110,00	-	Yes	ENISA
St. George Lyca-bettus Boutique Hotel	2, Kleomenous str.	3021074 16 000	98,00	-	Yes	ENISA
Amalia Hotel Athens	10 Amalias Ave.	3021032 37 300	90,00	100,00	Yes	2nd International Conference on Cyber Crisis
Airotel - Hotel Alexandros	105 Michala-copoulou Str.	3021064 00 720	69,00	79,00	Yes	ENISA
Airotel - Hotel Stratos Vassilikos	114 Michala-kopoulou	3021077 06 611	83,00	92,00	Yes	ENISA
Airotel - Hotel Parthenon	6 Makri	3021092 34 594	87,00	96,00	Yes	ENISA
Fresh Hotel	26 Sophocleus & Klisthenous	3021052 48 511	80,00	90,00	Yes	ENISA

Links to Athens guides:

www.athensguide.com - www.greece-athens.com - www.athensguide.gr

Folllow-up on ENISA on:

http://www.facebook.com/ENISAEUAGENCY
https://twitter.com/enisa_eu
https://www.youtube.com/user/ENISAvideos
http://www.linkedin.com/company/european-network-and-information-security-agency-enisa-

enisa
A EUROPEAN AGENCY

enisa

2nd International Conference on Cyber-crisis Cooperation and Exercises

23-24 September 2013
Athens, Greece

"European Union cyber-security agency ENISA invites public and private sector organisations look at how increased cooperation and security exercises can help to protect cyberspace from attacks and disruption."

Conference topics

- Cyber-security and crisis management exercises
  - → Emerging cyber-threats as cyber-exercise scenarios (supply chain integrity, DDOS, privacy, cyber-espionage)
  - → Large-scale cyber-exercises
  - → Simulation environments and visualisation techniques
- National NIS incident management and cooperation plans
- Alerting systems and information exchange platforms for cross-border NIS cooperation
- Integrated situational awareness
- Data collection, abstraction, visualisation
- Governance models, practices and escalation procedures for cyber crisis management
- International NIS cooperation for incident management and response
- Handling public relations and media in the case of major cyber-incidents
- Cooperation between cyber security and cyber defence stakeholders

http://www.enisa.europa.eu/ccce-conference

Address: Divani Caravel Hotel
Vasileos Alexandrou 2
Kesariani, Athens 16121, Greece
Tel. +30 210 7207000 | Fax +30 210 7236683 | info@divanicaravel.gr

www.enisa.europa.eu