1st International Conference on Cyber Crisis Exercices & Cooperation

Paris, June 27, 2012

Information Package

enisa
European Network and Information Security Agency

Table of Contents

1. Foreword from the Executive Director

As the Executive Director of ENISA I proudly welcome you to our first international conference on cyber crisis cooperation: cyber exercises. This conference focuses on cyber exercises as part of an ongoing effort to enhance network and information security and cyber crisis cooperation across the European Union.

The objectives of the *first international conference on cyber crisis cooperation: cyber exercises* are to exchange good practices in the field of international cyber crisis cooperation, specifically focusing on cyber exercises, bring together the stakeholders that organise and have experience in cyber exercises in order to explore cooperation between them, and identify gaps and challenges in the field of international cyber crisis cooperation and in particular on cyber exercises.

ENISA welcomes all participants: stakeholders and experts in the field of cyber crisis cooperation, and especially those with experience in organizing cyber exercises.

In addition to this conference, ENISA is carrying out a project regarding the stocktaking of national and international cyber exercises inside and outside the European Union. The project will result in a stocktaking report and a global map of cyber exercises. The outcome of the stocktaking and the conference will be used by ENISA in our effort to enhance cyber crisis cooperation in Europe.

I wish you all an inspiring day!

Prof. Udo Helmbrecht
Executive Director of ENISA

2. Program

09:00 - 09:25	Registration
09:25 - 9:30	Opening from the organizers
9:30 - 10:00	*Keynote speakers* **Evangelos OUZOUNIS, Head of Resilience and CIIP Unit, ENISA** **Ann-Sofie RONNLUND, DG Connect, European Commission**
10:00 – 11:00	*New World of Cyber Crisis and Exercises* Speakers: **Arjen BOIN** (Utrecht University) **Koki YOSHIDA** (NISC Japan) **Wolfgang ROEHRIG** (European Defence Agency)
11:00-11:15	Coffee break
11:15-13:00	*Cyber Exercises Case Studies* Speakers: **Reggie MCKINNEY** (DHS) **Susanne JANTSCH** (BSI Germany) **Martin GÜRTLER** (NATO/CCDCOE) **Derron STÉPHANE** (Federal Chancellery Switzerland) **Adrien OGEE**(ANSSI France) **Panagiotis TRIMINTZIOS** (ENISA)
13:00-14:00	Lunch Break
14:00-15:30	*Technical Aspects of Cyber Exercises* Speakers: **Chris C. DEMCHAK** (US Naval War College) **Diego Fernández VÁZQUEZ** (ISDEFE) **Miguel Ángel ABAD** (CNPIC) **Michael BILZOR** (US Naval Academy) **Daisuke INOUE** (NICT Japan) **Thierry BENOIST** (European Commission, JRC)
15:30-16:00	Coffee break
16:00-17:30	*Open session on the future of Cyber Exercises and Results of the ENISA International Stocktaking on Cyber Exercises* Moderators: **Panagiotis TRIMINTZIOS** (ENISA) & **Razvan GAVRILA** (ENISA)

3. Biography of Speakers

Keynote speakers

Name: Dr. Evangelos Ouzounis
Dr. Evangelos Ouzounis is the head of ENISA's Resilience and Critical Information Infrastructure Protection (CIIP) Unit. His unit implements EU Commission's CIIP action plan, organises CIIP exercises (e.g. Cyber Europe 2010, Cyber Atlantic 2011, Cyber Europe 2012), facilitates Member States' efforts towards a harmonised implementation of incident reporting (article 13a of new Telecom Package), and develops good practice for national cyber security strategies and national contingency plans. ENISA's Resilience and CIIP Unit runs also numerous other studies on cyber security aspects of critical sectors and services such as Industrial Control Systems - SCADA, Smart Grids, Cloud Computing and Interconnected Networks. The programme issues strategic recommendations and develops good practices for relevant stakeholders.

Name: Ann-Sofie RONNLUND,
Short bio: Ms Ronnlund is working for DG Connect at European Commission in the unit responsible for cyber security policies.

New World of Cyber Crisis and Exercises

Name: Prof. Dr. Arjen Boin
Title of the presentation: Preparing for transboundary crises: three challenges
Abstract: The new world of crisis is dominated by the rise of transboundary threats, which reach across geographic, political and policy boundaries. Cyber threats are a prime example of transboundary crises. These crises pose unique challenges that traditional response structures are ill equipped to deal with. In preparing for these crises, we have to pay attention to the traditional challenges of crisis management and how they play out in a transboundary context.
Short bio: Arjen Boin is a professor of public governance and crisis management at the Utrecht School of Governance and an adjunct professor at the Public Administration Institute, Louisiana State University. He received his

Ph.D. from Leiden University, The Netherlands where he taught at the Department of Public Administration. Professor Dr. Boin has published widely on topics of crisis and disaster management, leadership, institutional design and correctional administration. He serves on the editorial board of *Risk Management* (Palgrave) and the *Journal of Contingencies and Crisis Management* (Blackwell). He is the Editor for *Public Administration*, a premier journal in the field. He is also a managing partner of Crisisplan BV. Professor Dr. Boin is a founding member of the European Societal Security Research Group.

Name: Koki Yoshida
Deputy Counsellor for International strategy; National Information Security Centre (NISC), Cabinet Secretariat, Japan
Abstract: Japan has conducted cross-sectoral exercises with several critical infrastructure operators since 2006. Based on the lesson learned in the Great Japan Earthquake in March 2011, the NISC improved their exercises for complex critical infrastructure failure. The presentation also shares the lessons learned from the earthquake.
Short bio: Mr. Yoshida graduated from the University of Tokyo and received a Master's degree from the School of International Relations and Pacific Studies, University of California, San Diego. He joined the Ministry of Internal Affairs and Communications (MIC) in 2002. He has contributed to the policy development in the ICT area (TV program and web-contents promotion policy, trade negotiation such as WTO and FTA and amending Telecommunication Business Law).

Name: Wolfgang Röhrig
Title of the presentation: The human factor in cyber defence – requirements for technical training and exercise infrastructures
Abstract: The military requirements on Cyber Defence capabilities are to: prepare for, prevent, detect, respond to, recover from and learn lessons.
The human being is still one of the weakest links in Cyber Defence. To strengthen this link, training and exercises are key. European Defence Agency is currently conducting R&T research on the human factor in cyber defence and a training need analysis for the different actors in defending military information infrastructures. Aligned with that, EDA investigates the

requirements for technical training and exercise infrastructures. The presentation will provide an overview of a proposal to member states Ministries of Defence to establish multinational cyber defence training and exercises ranges and/or to federate existing capacities into a training network.
Short bio: Wolfgang Röhrig was born in 1966 in Troisdorf-Sieglar, Germany. In 1985 he entered the German Navy as Officer Candidate. In 1986, Mr. Röhrig commenced his University Studies at the Federal Armed Forces University in Hamburg (UniBwHH), where he graduated with the degree of Diplom-Kaufmann, which equals a Master of Business Administration, in 1990. Between 1990 and 2006, Mr. Röhrig occupied several posts in the German Navy as Operator and ICT conceptual specialist, including several operational deployments (NATO Operation "Sharp Guard", NATO Operation "Active Endeavour", Coalition Operation "Enduring Freedom"). From 2006 to 2010, he held the position of Senior ICT Staff Officer for maritime CIS at the Supreme Headquarters Allied Powers Europe (SHAPE), whilst in 2010 he became Senior CIS Staff Officer for national and international cooperation on Information Assurance and Cyber Defence at the German Armed Forces IT-Office (IT-AmtBw) in Koblenz, Germany. Since March 2012, Mr. Röhrig has been Project Officer Cyber Defence at the European Defence Agency in Brussels.

Cyber Exercises Case Studies

Name: Dr. Susanne Jantsch
Title of the presentation: Two aspects of exercising cyber incidents
Abstract: Business Continuity Management / Emergency Planning includes that the plans – once established – should be exercised. For organisations that have just started their emergency planning and that have little or no experience with exercises, “sample” exercises that can be adapted to the organisation’s needs may provide a tool to get into regularly exercising. And what happens when a cyber incident evolves into a crisis? In the second part of the presentation, an overview is given on LÜKEX 11, a large, biennial national crisis management exercise that in 2011 focused on cyber incidents. Cascading incidents were to trigger overarching national crisis management involving public administration

authorities at Federal and Länder level as well as critical infrastructure providers.
Short bio: Susanne Jantsch is senior cyber exercise expert and head of the exercise team at the Federal Office for Information Security (BSI). In support of the planning team of the Federal Office for Civil Protection and Disaster Recovery (BBK), she leads the BSI parts of LÜKEX planning. She has been involved in planning and performing cyber and CIP-related exercises since 1999.

Name: Martin Gürtler
Title of the presentation: technical cyber defence exercise: locked shield 2012
Abstract: The NATO CCD COE conducted a technical CD EX in 2012 together with several partners. The exercise took place over the Internet in a virtualized game scenario It required nine blue teams to defend their systems over two days against real-time attacks from a red team.
Short bio: LTC Martin Gürtler is the Chief of Staff and Deputy Director of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

Name: Stéphane Derron
Title of the presentation: HERMES OEx: guidelines for the design of exercises
Abstract: Exercises are fictitious and sometimes even somewhat abstract situations that must be carefully defined, planned and organised. For this purpose, a systematic project management method is useful to enhance the work efficiency and understanding of the project for everyone involved.
Short bio: Stéphane Derron Holds the Project management certifications PMP (PMI) and HSPTP (HERMES). He is Deputy Head of the Federal Crisis Management Training at the Swiss Federal Chancellery and in charge of the Strategic Exercise 2013.

Technical Aspects of Cyber Exercises

Name: Dr. Chris C. Demchak
Title of the presentation: "Games versus exercises: designing surprise-resilient organizations for a cybered world"
Abstract: The globally complex cyberspace substrate that introduces surprise into the lives of individuals directly and globally en masse today is changing conflict and security requirements across cyberspace's communities of civil and less civil societies. Transforming into cybered surprise-resilient organizations and nations requires adjustments in concepts of conflict, domain, war, cyber power, secure technological designs, and national resilience for security. To know how to go about these adjustments, one must rethink what can be learned about likely surprise using on-off major exercises which do not reflect the continuously iterative, generative, and dynamic behaviour of a truly cybered world and its conflicts. Rather, complexity theory's recommended 'discovery trial-error learning' (DTEL) requires continuously accessible, co-authored, operational, game-based simulations integrated into institutional knowledge-based structures such as the Atrium model presented here as an exemplar. The goal is better 'security resilience' across all the interlinked, critical socio-technical systems of a democratic nation.
Short bio: Dr. Chris C. Demchak is Co-Director of the Center for Cyber Conflict Studies and a Research Professor in the Strategic Studies Department at the US Naval War College. She has a PhD from Berkeley (political science) with a focus on organization theory and systems, security studies, and surprise in complex technical systems across nations. She also holds two masters degrees, respectively, focused on economic development (Princeton) and energy engineering (Berkeley). She has published numerous articles on societal security difficulties with large-scale information systems to include cyber conflict, privacy, and the rise of cyber Westphalian system, along with three books: Military Organizations, Complex Machines in the Cornell Security Studies series, Designing Resilience (2010, co-edit), and *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security Conflicts* (2011). She is currently working on a new manuscript tentatively entitled *Organizing for Cybersecurity: Cyber Commands and their National Equivalents in the Cybered Conflict Era*. Her research focus is the evolution in cybered organizations and

their tools, the implications for national cybersecurity/deterrence strategies, and organizational learning structures and techniques after experiences with cybered confrontations.

Names: Miguel Ángel Abad Arranz (CNPIC) and Diego Fernández Vázquez (ISDEFE)
Title of the presentation: Fostering awareness for the protection of the Control Systems in Critical Infrastructures - Spanish experience
Abstract: One of the strategic priorities to ensure security and safety for nations nowadays is the protection of their Critical Infrastructures (CI), which provides essential services for the normal operation of our societies. Taking into account that most of these CI are based upon information and telecommunication technologies (ICT), new threats arises that could jeopardize the protection level of the CI. ISDEFE (http://www.isdefe.es), in collaboration with the National Centre for Critical Infrastructure Protection CNPIC) of the Spanish Ministry of Interior (http://www.cnpic.es), has conducted the First PSCIC Technical Sessions in April 2012. The PSCIC workshop (https://www.jornadaspscic.isdefe.es/) was a series of practical sessions, nationwide and cross-sector, to reinforce and test the skill acquisition for the Protection of Control Systems in CI, as well as to assess their processes and procedures.

Name: Commander Michael Bilzor
Title of the presentation: Student Cyber Exercises, Large and Small
Abstract: In this talk, we will briefly describe two cyber exercises employed at the U.S. Naval Academy: one smaller and one larger.
The smaller exercise is experienced at the end of the Freshman course called Introduction to Cyber Security. This course was offered for the first time in 2011-2012, and as a core course, it is taken by all students, regardless of prospective major. The course culminates in three labs: a dedicated cyber defense lab, a dedicated cyber attack lab, and finally a lab in which defense and attack are combined.
The larger exercise supported by the U.S. Naval Academy is the annual Cyber Defense Exercise (CDX), which is administered each Spring by the National Security Agency (NSA). During CDX, students from nine military schools in the U.S. and Canada, at both the undergraduate and postgraduate levels, spend three days protecting a network, responding to attacks by an NSA 'red cell'

adversary team. Points are awarded for maintaining the availability of network services, and a trophy is awarded at the end of the competition.
We will explore the educational challenges of conducting small-scale cyber exercises, like the one in our Introduction to Cyber Security class, and participating in larger-scale cyber exercises, like CDX.
Short bio: Commander Bilzor is a military professor in the Computer Science Department at the U.S. Naval Academy in Annapolis, Maryland. He has logged over 2,000 flight hours in the F-14 Tomcat and the F/A-18 Super Hornet with the U.S. Navy. He received his Ph.D. in Computer Science from the U.S. Naval Postgraduate School in Monterey, California, in 2011. His primary research interest is in hardware and software security.

Name: Daisuke Inoue
Title of the presentation: Overview of NICTER - R&D project against cyber-attacks in Japan
Abstract: We have been developing the Network Incident Analysis Center for Tactical Emergency Response (nicter) - which is an integrated security system taking advantage of large-scale dark net monitoring, automated malware analysis and their correlation - in order to grasp the global trends of malicious activities over the Internet. This presentation will describe the current R&D activities on the nicter to fight against existing and emerging cyber attacks.
Short bio: Daisuke Inoue received a Ph.D. degree in engineering from Yokohama National University in 2003. He is the director of the Cybersecurity Laboratory in the National Institute of Information and Communications Technology (NICT), where he is involved in a Cybersecurity R&D project called “nicter”.

Name: Thierry Benoist
Title of the presentation: On the use of emulation test-beds for increasing the realism of operational cyber exercises
Abstract: The level of detection, coordination and response capabilities of Critical Infrastructure (CI) operators, e.g., Network Service Providers, are among the key factors that determine the impact of disruptions to the economy and society during a contingency. Furthermore Critical Infrastructures

are increasingly dependent on cyber technologies and thus vulnerable to cyber threats. In this context operational cyber exercises become invaluable preparedness activities. In order to address the challenge of recreating a realistic but strictly confined exercising environment the use of emulation test-beds, e.g. based on the "Emulab" software, is proposed as a platform to conduct operational multi-party cyber-exercises. The presentation shows: a) how an Emulab-based test-bed can be adapted to meet the requirements for such operational exercises and human-in-the-loop testing; b) how voice communication between players can be used during exercises by simulating a PSTN network; c) how an exercise can run using a feature-rich exercising interface that supports exercise moderators and players. Our experiences indicate that both at a theoretical and practical level, the use of emulation test-beds for the execution of operational multi-party cyber-exercises is a very promising approach that deserves further investigation and testing. Previously, Mr. Benoist had been responsible for classified IT activities of the IPSC for four years, and led several IT projects for the European Chemical Agency for more than three years.

Short bio: Dr Thierry Benoist is working for the European Commission where he is conducting research on cyber-security at DG-JRC in the Critical Infrastructure Protection action of the Security Technology Assessment Unit of the Institute for the Protection and Security of the Citizen.

Open session on the future of Cyber Exercises

Name: Dr. Panagiotis Trimintzios

Short bio: Panagiotis Trimintzios is working on Cyber Crisis Exercises and Cooperation within the Resilience and CIIP Unit at the Technical Department at the Network and Information Security Agency (ENISA), where he works since 2005. He was the manager of Cyber Europe 2010, the first pan European large scale cyber exercise, and of Cyber Atlantic 2011, the first EU-US cyber exercise. Currently, Dr Trimintzios is planning the second pan European exercise, Cyber Europe 2012 and also works in the area of cyber crisis cooperation and management. In the past he has worked in various areas on network and information security and published reports on Resilience Metrics, Resilience of the Internet Interconnection Ecosystem (Inter-X), and National Cyber Contingency Planning. 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 Data Networks and Telecommunications, a PhD on Network Quality of Service Management, while before 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.

Name: Mr. Razvan Gavrila
Short bio: Mr. Gavrila is a NIS Operations Officer at ENISA since Aug 2011. He is working on Cyber Crisis Exercises and Cooperation within the Resilience and CIIP Unit at the Technical Department. Before joining ENISA, Mr. Gavrila worked with the Romanian Computer Emergency Response Team (CERT) and the Ministry of Foreign Affairs.

4. Themes of the Conference

The conference themes for the **first international conference on cyber crisis cooperation: cyber exercises** are based on the objectives for the conference and divided in two main categories: what we exercise and how we exercise. The word ***'we'*** refers to all stakeholders involved in the field of cyber crisis cooperation and cyber exercises. A description of the different themes is provided below.

What we exercise

The first dimension of the conference theme of the **international conference on cyber crisis cooperation: cyber exercises** aims to discuss the need for cyber exercises in the context of enhancing cyber crisis cooperation. The topics in this dimension are:

1. **Transboundary crises: a need for large-scale cyber crisis cooperation**

Modern societies face the prospect of what we refer to as transboundary crises. These crises share some disturbing characteristics: transboundary crises unfold across borders and have widespread consequences; they are unusually complex and very hard to manage. Cyber crises are a type of transboundary crises and ask for large-scale cyber crisis cooperation. *(See Boin et al, 2008 and 2010)*

2. **Large scale cyber incidents analysis**

Analysis of large scale cyber incidents can help in the preparation on large crisis and cyber crisis cooperation. During the conference, we aim to discuss the different ways to analyse large scale cyber incidents.

3. **Challenges in cyber crisis cooperation and situational awareness**

Large-scale cyber crisis cooperation, focusing on the importance of critical infrastructure protection, started with the Y2K threat. Since that time several incidents (such as the power outage in Europe in 2006 and cyber attacks in Estonia in 2007), policy initiatives (such as the 2005 Green Paper and EU Digital Agenda) and exercises (such as the Cyber Europe series) have shaped the international field of cyber crisis cooperation. Cyber crisis cooperation is challenged in several ways, such as in information exchange, international cooperation, public-private partnerships, and prioritization of actions. During the conference, we want to identify the challenges in the field of cyber crisis cooperation.

4. **Cyber crisis cooperation strategies**

When we are aware of the challenges in the field of cyber crisis cooperation, we will be able to discuss during the conference the different strategies for cyber crisis cooperation.

5. **Organisation of cyber crisis cooperation**

In this conference, we look for good practices about the organisation of cyber crisis cooperation. The topics that can be discussed in this session are: secure communications, standard operating procedures, plans and protocols, national contingency plans, and CERT preparedness.

6. **Results and lessons learned of cyber exercises**

The results of cyber exercises influence large-scale cyber crisis cooperation. Cyber exercises have in common that they gather results and lessons learned for the future. During the conference we aim to exchange lessons learned and recommendations for large-scale and international cyber crisis cooperation and future cyber exercises.

7. **Good practices for effective exercises**

The first international conference aims to exchange good practices in order for planners to be able to prepare effective exercises in the future.

How we exercise

The second dimension of the conference theme of the **international conference on cyber crisis cooperation: cyber exercises** focuses on how we exercise. Cyber exercises are an important tool to assess preparedness of a society against natural disasters, technology failures and emergency situations. Exercises enable authorities to identify and address specific weaknesses, increase cooperation across the sector, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience. The following topics in this dimension appear especially relevant:

1. **Organization and planning of exercises**

The conference aims to answer the following questions: How are cyber exercises organised? What are the success factors in the organisation of cyber exercises? What are the challenges in organising cyber exercises? How do exercises need to be planned?

2. **Cyber exercise scenarios**

One of the main aspects of a cyber exercise is the scenario that is used during the exercise. During the conference we aim to discuss how scenarios need to be prepared, what are the challenges in writing scenarios, and what are good practices to take into account.

3. **Scalability issues in cyber exercises**

During the conference, we would like to discuss which scalability issues occur in cyber exercises and how the issues can be dealt with.

4. **Tools for managing cyber exercises**

Several exercise management tools are available for the preparation, execution and the evaluation of cyber exercises. Exercise organisers can make use of exercise planning tools, exercise software and infrastructure tools, exercise simulation tools, media simulation tools and exercise evaluation tools. The conference aims to identify best practices about the use of exercise management tools.

5. **Infrastructure simulation and visualisation**

In addition on the topic on tools for managing cyber exercises, we would like to have an in-depth discussion on infrastructure simulation and visualisation tools.

6. **Monitoring and evaluation methods of cyber exercises**

Academic research has shown there is a need for structured evaluation in order to improve the learning of participants in exercises. Looking at outcomes of an exercise alone tends to undermine the aims of the exercise, is generally unfair to participants and feeds risk-avoiding behaviour. The focus should be on process characteristics that enhance the effectiveness of cyber crisis cooperation. Monitoring and evaluation tools help to structure feedback and select lessons learned. This session will discuss how monitoring and evaluation of cyber exercises is best organized in order to accomplish the aims of a large-scale cyber exercise.

During the conference, the themes of the conferences will be discussed in four sessions, following the key note speakers. These four sessions are:

- New world of Cyber Crisis and Exercises
- Cyber Exercises Case Studies
- Technical Aspects of Cyber Exercises
- The future of Cyber Exercises and results of the ENISA International Stocktaking on Cyber Exercises

The four sessions aim to target all conference themes as mentioned above.


27 JUNE 2012
PARIS
HOW TO REGISTER
WWW.ENISA.EUROPA.EU
1ST. INTERNATIONAL CONFERENCE
ON CYBER CRISIS COOPERATION:
CYBER EXERCISES
CALL FOR PAPERS
WWW.ENISA.EUROPA.EU
THE OBJECTIVES OF THE CONFERENCE ARE:
A) EXCHANGE GOOD PRACTICES IN THE FIELD OF INTERNATIONAL CYBER CRISIS COOPERATION, SPECIFICALLY FOCUSING ON CYBER EXERCISES.
B) BRING TOGETHER THE STAKEHOLDERS THAT ORGANISE AND HAVE EXPERIENCE IN CYBER EXERCISES IN ORDER TO EXPLORE COOPERATION BETWEEN THEM.
C) IDENTIFY GAPS AND CHALLENGES IN THE FIELD OF INTERNATIONAL CYBER CRISIS COOPERATION AND IN PARTICULAR ON CYBER EXERCISES.
MORE INFORMATION
WWW.ENISA.EUROPA.EU
enisa
European Network and Information Security Agency

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu