Report on the Second International Conference on Cyber-crisis Cooperation and Exercises

October 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Panagiotis Trimintzios and Razvan Gavrila, ENISA

Contact

For more information about this document, please contact:

- Email: c3e@enisa.europa.eu
- Internet: http://www.enisa.europa.eu/c3e

Acknowledgements

ENISA would like to express its gratitude to the speakers and participants in the **Second International Conference on Cyber-crisis Cooperation and Exercises**. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity. ENISA would also like to thank Deloitte for supporting this project.

ISBN 978-92-9204-071-0 doi: 10.2824/2584

Table of Contents

1 Introduction

In 2012, ENISA organised the first international conference on cyber-crisis exercises and cooperation.[1] Following the success of this event, ENISA hosted the '**Second ENISA International Conference on Cyber Crisis Cooperation and Exercises**' on 23–24 September 2013 in Athens, Greece which comprised a variety of contributions and panel discussions covering the key challenges and developments relating to cyber-crisis cooperation and exercises.

The objectives of the Conference were:

a) to exchange good practices in the field of international cyber-crisis cooperation and cyber exercises;
b) to bring together the stakeholders that organise and have experience in cyber-crisis cooperation and cyber exercises in order to enable/enhance cooperation between them; and
c) to identify gaps and challenges in the field of international cyber-crisis cooperation and in cyber exercises.

The **Second ENISA International Conference on Cyber-Crisis Cooperation and Exercises** was a unique high-profile international event that aimed to directly support the new cyber security strategy[2] of the European Union by helping various constituents in their efforts to establish a more coherent cyber security policy. Additionally, the conference was a key knowledge sharing platform for national and governmental level cyber security experts. It also facilitated debate and information exchange, and offered networking opportunities to both technical experts and executive stakeholders.

The event presented an excellent opportunity for the participants to share thoughts, opinions and expertise in the field of cyber-crisis cooperation, focusing on topics such as:

1. Cyber security and crisis management exercises
2. National NIS incident management and cooperation plans
3. Alerting systems and information exchange platforms for cross-border NIS cooperation
4. Integrated situational awareness. Data collection, abstraction, visualisation
5. Governance models, practices and escalation procedures for cyber-crisis management
6. International NIS cooperation for incident management and response
7. Legal aspects of NIS cooperation and information sharing
8. Handling public relations and media in the case of major cyber-incidents
9. Breach notification / regulatory affairs: ENISA as the reporting point for the Member States
10. Cooperation procedures involving civilian and national security stakeholders

The conference achieved its objectives and succeeded in creating an open and collaborative platform for sharing experience and insights between the 120+ participants. Moreover, leveraging on the success of the **Second ENISA International Conference on Cyber-Crisis Cooperation and Exercises,** the Agency aims to continue organise follow-up actions and is considering a third such conference in the years to come.

[1] More information is available at: http://www.enisa.europa.eu/c3e/conference

[2] See also the EU Cybersecurity plan to protect open internet and online freedom and opportunity – Cyberecurity 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

2 Agenda

The conference speeches were grouped under nine major themes. The individual presentations of the speakers are available online on the website of the Conference: http://www.enisa.europa.eu/ccce-conference

Day 1 – 23 September 2013
Keynote: Prof. Udo HELMBRECHT, Executive Director, ENISA
Session 1: Governance models, practices and cooperation procedures for cyber-crisis management **Chair: Iowa CARELS, National Cyber Security Centre, The Netherlands**
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 RONNLUND, 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***
Session 2: Cyber-crisis management and cooperation exercises **Chair: Rob HARRIS, Cyber Security Operations Centre (CSOC), UK**
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***
Session 3: Governance models, practices and cooperation procedures for general crisis management **Chair: Helena RAUD, National Information Systems, Estonia**
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***
Panel Session: Cyber-exercise scenarios: supply chain integrity **Chair: Demosthenes IKONOMOU, ENISA**
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, Ericsson – *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***

Day 2 – 24 September 2013
Session 1: Opening speeches **Chair: Panagiotis TRIMINTZIOS, ENISA**
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'***
Session 2: Issues on cyber security crisis management, cooperation and information exchange **Chair: Paul RHEIN, Haut-Commissariat à la Protection Nationale, Luxemburg**
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: So-Jeong KIM, National Security Research Institute, S. Korea – *Cyber-security in the Republic of South Korea***
Session 3: Technical issues on cyber-crisis cooperation and exercises **Chair: Andrea DUFKOVA, ENISA**
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***
Session 4: Infrastructures related to cyber-crisis cooperation and exercises **Chair: Razvan GAVRILA, ENISA**
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***
Panel Session: Challenges and approaches of cyber risk assessments **Chair: Neil ROBINSON, RAND Europe**
Speaker 1: Panagiotis TRIMINTZIOS, ENISA – *ENISA 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*** **Speaker 4: So-Jeong KIM, National Security Research Institute, S. Korea – *Cyber-security Risk Assessment in South Korea***
Closing remarks – Panagiotis TRIMINTZIOS, ENISA

3 Conference facts and figures

In order to illustrate the coverage and the relevance of the conference, we include below some statistics and figures from the event.

- More than 75 different organisations participated in the conference
- Around 200 people registered to participate to the conference, of which 120 were invited (due to limited places); they came from 30 different counties
- 31 experts from different fields, including cyber exercises specialists, crisis managers, risk managers, etc., were involved in the conference programme
- Around 20 large ICT and cyber security companies were present at the event

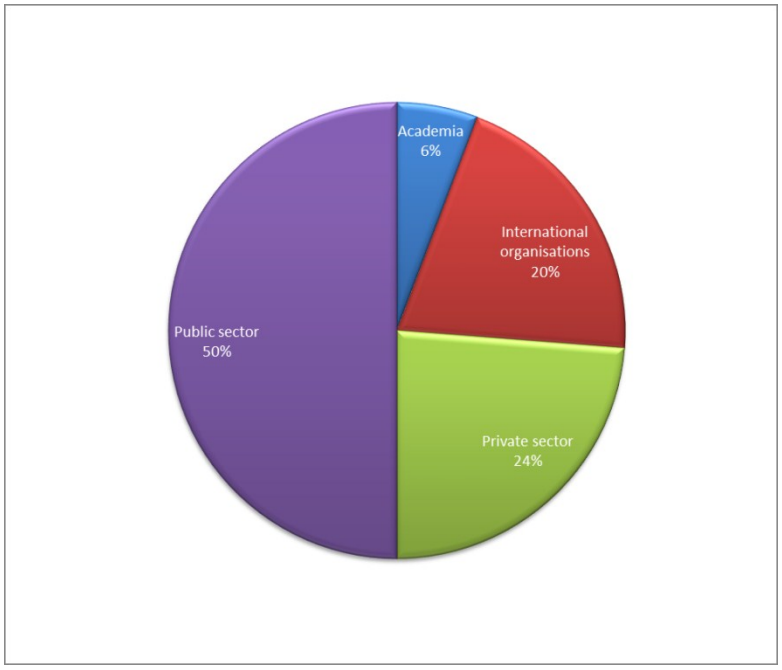


Figure 1: Overview of participants

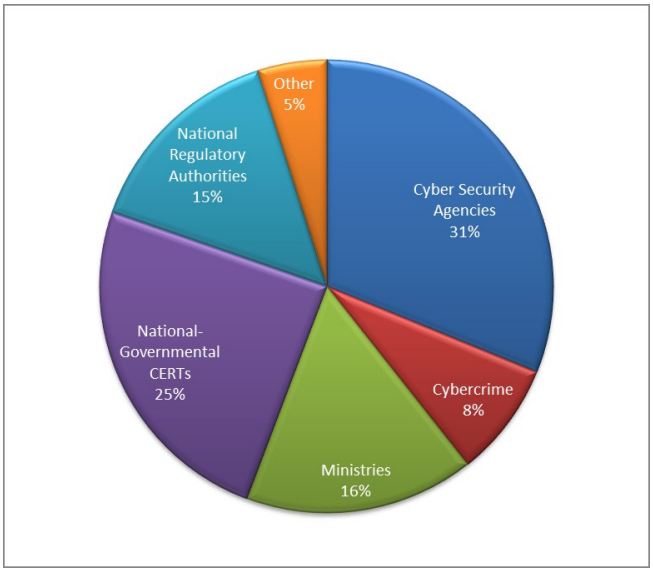


Figure 2: Public sector participation

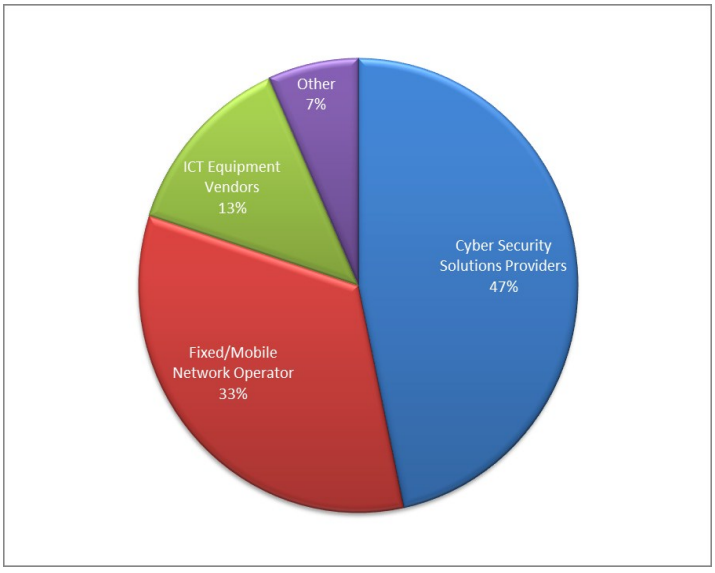


Figure 3: Private sector participation

4 Conference key messages and insights[3]

The keynote speech by ENISA's Executive Director, Prof. Udo Helmbrecht, provided an overview of the related policy initiatives in the European Union. The speaker gave a summary of the relevant work of ENISA and the European Commission in the field of cyber-crisis cooperation and cyber exercises. He also gave an overview of the key elements of the European Union's Cyber Security Strategy and its overall relevance for the Member States' economy and society.

The conference included eight sessions. Below we summarise the key messages, the insights and the comments by the speakers, the panellists and the audience during these sessions.

4.1 Governance models, practices and cooperation procedures for cyber-crisis management

The first session of the conference introduced a set of viewpoints on cooperation models during a large-scale cyber-crisis. The lessons learned from prior cyber-crisis exercises indicate that a valuable governance model for the crisis management activities is a well-established and effectively implemented **formal advisory board** in which the stakeholders should work together closely during a cyber-crisis.

Information sharing and analysis within such a formal advisory board provides better strategic guidance during the mitigation phase of the crisis, shaping the decision-making process. A crucial point highlighted during the discussions was that such a group should encompass various fields of expertise and should also be constantly 'nurtured' via informal meetings and exercises.

A presentation on existing activities for developing crisis cooperation frameworks at EU level emphasised the need for a layered approach. The European Cyber-Crisis Cooperation Framework (ECCCF) is a strong procedural triple-layer framework for cooperation between EU public organisations – supporting the Member States' needs. The ECCCF defines generic crisis management functions for each of the following three layers:

- technical,
- operational, and
- strategic/political.

In particular, the technical layer of the ECCCF provides for the key assumption that although there is still room for improvement, the cooperation and information exchange procedures in place between national structures involved, e.g., Computer Emergency Response Teams (CERTs) are robust. It has been determined that CERTs have long-standing information exchange channels or at least understandings that work sufficiently well for them to know how to pass to one another the relevant and actionable information, especially in the case of a large-scale cyber-incidents.

At the operational level the EU cyber community is still in the capability-building phase. The recent pan-European cyber exercises[4] indicate that this community should focus on: the threat analysis, situational assessment and mitigation action measures. Cyber security agencies, CERTs, IT ministries, regulators, communications authorities, etc., will all need to increase their efforts in adopting in their daily work the EU Standard Operational Procedures (SOP), written by and for EU cyber security crisis managers. These provide a set of good practices to improve information exchange and

[3] Note that this report is not a full summary of all presentations. The latter are available to download at the website of the event: www.enisa.europa.eu/ccce-conference
[4] Visit: www.enisa.europa.eu/c3e

cooperation at operational level between countries during multinational cyber-crises, in order to speed up the understanding of their causes and the mitigation of their impacts.

From an EU perspective it is relevant to highlight that at the strategic/political level there are **already existing European crisis management procedures,** namely the EU integrated political crisis response arrangements (formerly known as crisis coordination agreements). Although they do not explicitly cover cyber-crises, these crisis management procedures are generic enough to meet any crisis, including cyber. On the other hand, it is acknowledged that the existence of cooperation frameworks and mechanisms does not by itself ensure positive cyber-crisis outcomes. The pan-European cyber exercise, Cyber Europe 2014, will focus on exploring the crisis cooperation mechanisms of all layers.

The first theme of the ENISA conference also gave insights into the preparedness response to the cyber security challenges from the United States perspective. An interesting insight was provided into actions undertaken by NIST in order to work with the relevant stakeholders for jointly developing a **voluntary framework for reducing cyber risks** to critical infrastructure – in response to the national US policy reflected by the US Executive Order 13636 on improving critical infrastructure cyber security.

This US voluntary cyber security framework is being developed in an open manner with input from stakeholders in industry, academia and government, including a public review and comment process, workshops, and other means of engagement. The cyber security framework is intended to be leveraged by organisations looking to establish or improve a cybersecurity programme, to communicate cyber security requirements with stakeholders and/or to identify gaps.

All the above viewpoints were complemented by the European Commission's views and initiatives reflected in the **European Cyber Security Strategy** and in the draft **Directive on Network and Information Security**.

The session also revealed the importance of public–private partnerships when it comes to responding effectively to cyber-crises. An excellent example is the partnership in the Netherlands that has proved useful both during real cyber-crisis incidents, and also before such incidents through its risk assessment and mitigation measures.

4.2 Cyber-crisis management and cooperation exercises

The second session of the conference stressed the importance of having the right expectations set prior to performing cyber-crisis exercises. Techniques used by cyber adversaries are continuously evolving – techniques which **incorporate innovative elements**, starting from the use of popular websites for information gathering, steganography[5] and aggressive identity theft techniques, combined with the use of massive resources, both technical and human.

Several lessons learnt from real-life cases were presented, illustrating the value of **cyber intelligence sharing** with private industry and national CERTs as well as the usefulness of information sharing platforms and information exchange standards.

The presenters also highlighted the importance of cross-layer cooperation, for instance linking the policymakers to technical people and vice versa, in particular during national cyber exercises. A popular view amongst the conference participants was that nation-wide cyber-crisis management

[5] A general term to describe techniques for hiding messages within otherwise legitimate/normal ones.

and cooperation exercises are key in strengthening society's ability to manage national IT-related crises, primarily by developing the capability for public and private actors to cooperate and coordinate with one another.

Key characteristics of the cyber-crisis management and cooperation exercises were emphasised by the speakers. Depending on the amount of effort invested by organisations, such exercises can provide 'pressured' situations as close to reality as one would feel during a crisis. Setting such ambitious goals requires persistence and continuous improvement.

The main acknowledged benefits of the exercises could be summarised as follows:

- Enhancement of participants' capability in analysing consequences and response measures
- Obtaining an increased knowledge of 'available' resources for cyber-crisis management
- Preparation of alternative platforms for communication in case of a large-scale cyber-crisis or threat
- Creation of the opportunity to immediately update cyber-preparedness policies, plans and processes.

Since a cyber-crisis situation can only be resolved by cooperation and information sharing, special emphasis was placed on the mutual benefits achieved by the participants in multinational and multilevel cyber exercises in terms of ensuring preparedness. However, it was acknowledged that despite good preparation and collaborative approaches, such exercises may not always reach their objective to initiate real information sharing and multinational collaboration between participating nations. Expectations of such collaboration should be realistic and well balanced with the actual level of contribution from each party involved.

4.3 Governance models, practices and cooperation procedures for general crisis management

The third session of the conference brought to the audience the key lessons learned from crisis management and cooperation in domains that are significantly different from the cyber security domain. The session made obvious to all the many conceptual similarities in crisis management in classic areas such as public health, disease prevention and control, aviation and air traffic management. One particular example is the early warning and response system and intelligence information systems used for disease prevention and control in order to ensure cooperation and adequate management of crises. Inspirational examples of how the public health threats are detected and reported and on how (rapid) risk assessments are undertaken can be further extrapolated for the cyber security domain. It is clear that the story of one industry's challenges and how it overcame the adversities and applied the lessons learned can often be conceptually 'cloned' to the cyber security domain too.

Another practical example of a crisis management and coordination mechanism that is comprehensive in nature (covering a cyber dimension too) came from the aviation sector, air traffic management in particular. In this example, the key actors involved have clearly acknowledged the high relevance of the cyber-crisis elements, and supported the execution of a specific cyber exercise (codenamed 'Cyber13' cyber security exercise) in order to effectively test the governance models, practices and cooperation procedures. Amongst the key lessons learned, we highlight the following:

- Reporting lines on cyber issues need to be clarified
- Development and use of crisis management support tools is essential in order to ensure effective cooperation

- Crisis management procedures should be kept flexible, so out-of-the box solutions can emerge
- Country-level points of contact (Focal Points) should play a key role in the coordination and communication during major cyber events, involving national-level cyber security expertise, in addition to the EU-level one.

The recently established European Cyber Crime Centre (EC3) that is operational within Europol has a key role in fighting cyber-crime. The discussion focused on the benefits of tackling in a coordinated manner the collateral significant threats of ever-increasing cyber criminality.

These examples emphasise that – in line with the prior experience of other sectors – building an effective cyber-crisis management community is an intensive, sustained and time-consuming process, which takes time to mature. The advantage, though, is that cyber-crisis management communities can learn a lot from more traditional crisis management experiences in other areas.

4.4 Cyber-exercise scenarios: supply chain integrity

The session closing the first conference day provided insights into the good practices used in the private sector to appropriately safeguard the integrity of the supply chain, in particular within the telecommunications and information technology sectors.

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 have responded to these concerns by developing standards addressing various aspects of supply chain integrity. Moreover, organisations in various industry segments have developed best practices to deal with international suppliers and global supply chains.

The good practice approaches and concepts applied in the traditional supply chain integrity can be also adapted to the cyber domain as well. A key prerequisite is that there is a need for a coordinated general framework that unifies these ideas, as well as for more efforts from the standards bodies and industry associations.

Various types of crises that may impact the supply chains were illustrated, including (specifically) cyber-crises – with a view that preparedness, availability of resources and development of capabilities are key for successfully overcoming them.

Another interesting topic was the need to find the right balance between an open- versus closed-source model of approach in the supply chain (technology and software, in particular). There is a clear need for a framework to support a trusted supply chain for software and technology components that have relevance to, for example, critical (ICT) infrastructures, governments, and public services.

4.5 Issues in cyber security crisis management, cooperation and information exchange

During the fifth session the conference participants had the opportunity to learn about the cyber security situation in parts of the Asia-Pacific region. It showed that cyber-attacks can be motivated by cultural and political influences and agendas. Details were shared with the audience on certain patterns observed in the mechanisms by which these massive cyber-attacks emerge.

A set of interesting observations and correlations emerged from the monitoring and analysis of several relevant cyber-attacks noted in the Asia-Pacific region, as for example:

- It is relatively difficult to grasp activity trends using automatic monitoring tools;
- Sharing cyber-attack tools has become an extremely common trend, therefore the impact of simultaneous attacks by users without extensive knowledge or skills about cyber-attacks has increased significantly;
- Some Asia-Pacific countries, such as Japan, are mainly focused on building framework and strengthening the systems. The focus is on 'protection' rather than on 'response'.

A key catalyst of the cyber security management and information exchange process is adequate cyber-incident reporting. Such reporting, carried out after the incident has been resolved, helps us understand threats, vulnerabilities and the impact of incidents. Therefore, there is a strong opinion that incident reporting is vital to improve risk assessment, and to allow industry and government to improve cyber security.

During this session, ENISA gave an overview of the different types of incident reporting legislation in the EU and facilitated a discussion with the audience on how to set up an efficient and effective framework of incident reporting across Europe. Finally, there was a discussion of the impact of European legislation translated into actual measures – ENISA provided highlights on the security processes and information flows of the Telecom reform in Article 13a.[6] Of high relevance here was the information on the reporting tools available.

4.6 Technical issues in cyber-crisis cooperation and exercises

This session provided insight into the increasing professionalisation of technical cyber exercises and the possibility of gaining experience through 'lessons learned'. Examples included the competitive element of the Locked Shields competition, and the cyber security drills for the energy sector in Qatar. This also indicated that both developed and emerging economies are faced with the same set of cyber threat categories and each has to find its own measures in order to safeguard both national and trading interests.

One of the conclusions during the session was that one key success factor in good preparation of the national or regional cyber exercises is ample training and prior preparation. Another key success factor is a strong incentive to organise and participate in sectoral, national or regional cyber exercises where the 'nobody is left behind' principle prevails. Transparency, realistic participant expectations, mutual respect and active contribution to the exercises are other key elements.

An interesting presentation and analysis was made on the series of Distributed Denial of Service (DDoS) attacks targeting web services in the Czech Republic in March 2013. The series of cyber-attacks were well prepared in terms of planning, selection of the targets, good order of the targets, volume of the attacks and methods used for attacks. Despite the challenge raised by the attacks themselves, this situation was very enlightening for the Czech Republic and its Internet community – lessons were learned, technical information exchanged and the cyber-crisis cooperation mechanisms were further strengthened at national level. The presentation gave an overview of the attack and what type of solution and defence mechanisms were used to mitigate it. The participants were also informed about the process of information sharing and assessment and on the role and actions of existing Czech CERT/CSIRT teams during the attacks at national and international levels. The positive

[6] See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF and https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting

and also negative outcomes from this situation were presented, including key observations and changes made as a result of this event in the Czech Republic.

The importance of cyber-crisis exercises like Cyber Europe 2012 was highlighted as extremely valuable in enabling those concerned to respond effectively during the major incident in the Czech Republic.

4.7 Infrastructures related to cyber-crisis cooperation and exercises

The seventh session of the conference demonstrated the ever-increasing complexity of cyber security and the importance of infrastructures and professional training of cyber security experts – with the participants noting that the solid knowledge and skills of these experts represent a key asset. It was predicted that in the next decade skilled and competent cyber defence personnel will be a scarce and expensive resource – both in Europe and worldwide. In this context, it is relevant to highlight that the Defence part of the EU cyber security strategy emphasises awareness, skills and training.

The European Defence Agency (EDA) 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 provided the impetus to pursue several work strands, including cyber defence training and awareness to improve cyber resilience of future operations. EDA's presentation addressed training-related findings of its stocktaking study and gave insights on current training, exercises and awareness activities.

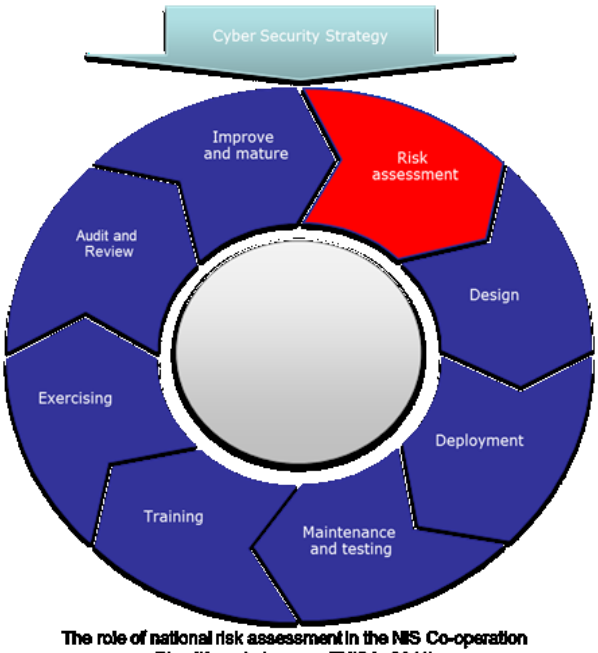
Complementing these views, but still in the same area of the cyber knowledge and skills as a fundamental 'infrastructure' asset, ENISA gave the participants a fresh overview of the on-going initiatives with regard to technical training for CERTs. Emphasis was placed on the need for a variety of types of training to respond to different requirements including legal, operational, technical and cooperation aspects for CERTs. The key success factor for such training is that it must be specifically tailored to fulfil the needs of this specific audience.

A fresh insight was presented by the European Commission on the Testa New Generation (Testa NG) communication platform that aims to support the exchange of electronic data between European and Member States' administrations in a secure, reliable and efficient way. The need and expectation for additional security levels and services that should be on top of the current network security architecture was a main driver for Testa NG.

A key challenge mentioned for the further roll-out of secure infrastructures (of the magnitude of Testa NG) relates to the legal requirements with regard to the handling of EU Classified Information (EUCI) within EU Member States, third countries and international organisations.

4.8 Challenges and approaches of cyber risk assessments

The final session of the conference concentrated on illustrating the key trends and practices for preparing National Risk Assessments (NRA) in the context of the lifecycle of National Contingency Plans (NCPs). [7] Such activities are aimed at identifying risks and assessing the impacts of potential incidents. As an overall contextual element, it is relevant to mention that in the **Cybersecurity Strategy for the EU** and the accompanied **proposed NIS Directive** [8] the European Commission specifically call for the development of national contingency plans (see for example Article 5 of the proposed NIS Directive) and for regular exercises testing large-scale networks' security incident response and disaster recovery, as a step towards closer pan-European coordination.



The role of national risk assessment in the NIS Co-operation Plan lifecycle (source: ENISA, 2011)

ENISA has carried out extensive work on national plans relevant to cyber security, and highlighted a number of interesting aspects and inspirational examples related to the applied national-level methodologies. For instance, the fact that most countries use scenario-based approaches where actors are gathered together to consider threat scenarios and impacts, or that most of the approaches to the conduct of an NRA are based on a decentralised model where each actor prepares their own risk assessment to be integrated by a coordinating authority.

Challenges noted were presented too, in particular:

- The lack of a harmonised national framework for cyber security, particularly terminology
- The incomplete and diverse risk assessment methodologies used
- Lack of comprehensive methods to address identified cyber threats
- Need for effective risk management and preparedness capacity and skills
- Need to establish and share a catalogue of scenarios to help the EU Member States in their NRAs.

In this context, it was recommended that there should be greater exchange of knowledge about risk analysis expertise with other domains that assess complex cross-border risks, such as border security financial services or public health, and to further facilitate access to EU scientific expertise on NRA.

An EU Member State presented insights on the steps taken towards a National Cyber Risk Assessment, revealing that this exercise helped in the identification and prioritisation of critical

[7] See the ENISA 2011, study on National Contingency Plans www.enisa.europa.eu/c3e/nis-cooperation-plans

[8] 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013' and 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final - 7/2/2013'. Both available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

information infrastructures and provided a very solid basis for a comprehensive National Contingency Plan. Moreover, it provided valuable input to several national cyber security strategy actions and complemented the national risk assessments in other areas.

Another interesting viewpoint was also presented from an US perspective – where the speaker highlighted the need to overcome legal barriers before rolling out best practices on cyber risk assessments from the governmental to private sector. This example also showed that the size of the country and the relative number of actors involved is not important when it comes to having a strong resolve to face the cyber security conundrum.

In 2013, ENISA will release an analysis of the existing practices in the area of National Risk Assessment. This document will be the basis of a pilot programme which will support Member States in developing comprehensive risk assessment capabilities. Similar activities have supported EU Member States in their efforts to set up National Contingency Plans for CIIP.

5 Main conclusions

In this section we summarise the high-level conclusions[9] of the conference, based on the presenters' opinions, the presentations and feedback from the audience. These high-level findings will further support and enhance cyber-crisis management and cooperation in Europe.

- The international community in cyber-crisis management, cooperation and exercises should be supported further through the provision of similar opportunities to ENISA's series of International Conferences. In addition to the discussions sparked by the presentations made by the different speakers, such an event provides for **excellent networking opportunities**. These types of networks are of paramount importance for effective cross-border cyber-crisis cooperation.

- **Cyber-crisis exercises** provide an excellent way to test and maintain cooperation procedures, plans and structures for dealing with large-scale crises. Ideas and knowledge in this area should be exchanged as far as possible and efforts should be aligned with each other, at national and international levels. Such exercises should be complemented with technical cyber security training that focuses mainly on skills development.

- There is a strong call for **better cooperation within and between public and private** sectors as the challenges faced by both private and public are strikingly similar. Not only should cooperation be an initiative worth pursuing, but best practices of both sides ought to be shared and learned from.

- It was noted that there are **numerous public initiatives that perhaps should align** in terms of objectives and activities, prior to linking up with both private enterprises and solutions.

- It is essential to have the right people at the table who can speak a **common language**. Technical experts and policymakers should meet in a neutral environment and find a way to talk a common language to bridge any differences and work out constructive solutions.

- The important decision on **full disclosure** to the public in the event of a crisis (and the potential counter-productive reaction of the public as well as giving the attackers tactical

[9] The order of this list does not suggest any priority in the activities to be undertaken.

knowledge on the progress of the defensive side) versus **covert cooperation** remains a balancing act. Many difficulties and intricacies make a one-size-fits-all solution impossible. The stakeholders seemed to agree that every organisation should make this decision for itself in order to find the right fit.

- There should be a balance between the focus on building cyber capabilities versus the focus on building a framework and strengthening the system. Both the 'Protect' and the 'Respond' strategies may be equally valid.

- There is an expectation to create a **security accreditation** scheme of infrastructure elements (supporting cyber cooperation), while it is acknowledged that accrediting such networks is neither necessary nor sufficient for building trust.

- In the next decade **skilled and competent cyber personnel** will be a scarce and expensive resource – both in Europe and worldwide. The ever-increasing complexity of cyber security emphasises the importance of professional training of cyber security experts. Technical cyber security exercises will help in this area.

- **Public–private partnerships** to develop valid scenarios and assess their impact on services and infrastructures are the recommended way forward to perform national-level risk assessments, depending on the specifics of each country. The actors involved should not hesitate to **seek guidance and obtain good practices** from other countries or European organisations.

5.1 Recommendations for future Conferences

Below are some recommendations for the future conferences on Cyber-Crisis Cooperation and Exercises:

- Future events should move in the direction of focusing on specific topics in the area of Cyber-Crisis Cooperation and Exercises. The focus could be associated with the location of the event. For example, a future conference hosted in a non-EU country could focus on international cooperation on exercises.
- The private sector should have a clear stand in the future conferences, focusing on their role in cyber-crisis cooperation but also on potential threats and scenarios for exercises in the private sector.
- Partnerships should be sought for future events. For example, synergies with other established events, collaboration with and sponsorships from the public and private sector stakeholders, etc.


enisa
A EUROPEAN AGENCY
INTERNATIONAL CONFERENCE on Cyber-crisis Cooperation and Exercises
enisa
2nd International Conference on Cyber-crisis Cooperation and Exercises
23-24 September 2013
Athens, Greece
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
"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."
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

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilisis Sofias
151 24, Marousi, Athens, Greece

doi: 10.2824/2584

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu