ENISA's efforts on Cyber Exercises

Policy Context

In the context of its i2010 Program, the European Commission issued a strategy for a secure information society highlighting the importance of dialog, partnership and empowerment. The policy debates paved the way for the CIIP Communication in 2009 "Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience". Among the actions proposed in this communication are steps to develop principles and guidelines for Internet resilience and conduct pan-European exercises on large-scale network security incidents and prepare a framework and a roadmap for European participation in global exercises.

The CIIP communication acknowledged that simulating incidents and running exercises to test response capabilities are strategic in improving the overall security and resilience of Critical Information Infrastructures. The European Commission invited Member States to develop national contingency plans and organise regular exercises for large scale network security incidents response and disaster recovery, as a step towards closer pan-European coordination.

The Tallinn Ministerial Conference, which took place in April 2009, built on the five pillars of the CIIP Action Plan and stressed that: "A joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan".

As a final ratification of the importance of exercising, at national but also at a pan-European level, the Council Resolution published in December 2009 mentions that: "Member States should organise national exercises and/or participate in regular European exercises in the area of Network and Information Security..." and that "...ENISA participate[s] with Member States on exercises to provide appropriate responses to emergencies...".

ENISA has engaged in being a facilitator for Member States by supporting the exchange of good practices in this area. In 2009, ENISA published a 'Good Practice Guide on National Exercises' with the aim to assist European stakeholders to design, plan, execute and monitor a national exercise on the resilience of public communication networks.
Supporting EU-wide cyber security preparedness exercises is one of the main actions of the Digital Agenda for Europe.

In this context, ENISA is facilitating the process of planning, conducting and evaluating pan-European exercises. The first such effort was the first pan-European exercise on CIIP, Cyber Europe 2010, conducted on 4 November, 2010. The exercise was organised by EU Member States with support from the European Network and Information Security Agency (ENISA) and the Joint Research Centre (JRC). Also, ENISA was the driving force behind the first EU US cyber exercise Cyber Atlantic 2011.

In 2012 ENISA facilitated the second pan European cyber security exercise, called Cyber Europe 2012, which has set more ambitious objectives and it is foreseen that it will further develop trust and cooperation of key actors in Europe in the area of CIIP.

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. In February 2013, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy announced the Cybersecurity strategy of the European Union. The importance of cyber-security exercises is further amplified as a result of this strategy and the accompanying Proposed Network and Information Security Directive.

ENISA's new mandate also highlights the importance of cyber security preparedness exercises in enhancing trust and confidence in online services across Europe.

Leveraging on the lessons learned from Cyber Europe 2010 and 2012, EU and European Free Trade Association (EFTA) Member States in collaboration with the EU Agency ENISA have developed the EU-Standard Operational Procedures (EU-SOPs), published in February 2014. The objective of the EU-SOPs is to aid in the response to major cyber incidents which can escalate to a cyber-crisis.

ENISA is currently planning with the EU Member States and EFTA countries the third pan European Exercise, Cyber Europe 2014. The EU-SOPs will be primarily tested during the second phase of Cyber Europe 2014. Cyber Europe 2014 builds on and ties together the extensive activities in the EU, at both national and European level, to improve resilience of critical information infrastructures.

Cyber Europe 2010

ENISA facilitated the first ever pan-European Exercise, Cyber Europe 2010. The exercise was conducted on 4 November, 2010. Its objective was to trigger communication and collaboration between countries to respond to large-scale cyber-attacks. Over seventy experts from the participating public bodies worked together to counter more than three hundred simulated hacking attacks aimed at paralysing the Internet and critical online services across Europe. During the exercise, a simulated loss of Internet connectivity between the countries took place, requiring cross border cooperation to avoid a (simulated) total network crash.

ENISA issued the final report on Cyber Europe 2010. The report underlines the need for:

- more cyber security exercises in the future,
- increased collaboration between the Member States,
- The importance of the private sector in ensuring security.

More information about Cyber Europe 2010:
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010

Cyber Atlantic 2011

An EU-US Working Group on Cyber security and Cyber Crime (EU-US WG) was established in the context of the EU-US summit of 20 November 2010 in Lisbon. The Cyber Atlantic exercise is a result of the EU-US cooperation within this working group (WG). Cyber Atlantic 2011 was delivered on 3 November, 2011 as a centralised table-top exercise, with over sixty participants from sixteen EU member states and the US.

Each participating country was represented by two players and one country moderator. The country moderators facilitated the work of his/her players, and had, among other things, the responsibility of distributing the scenario injects as decided by the exercise moderators.

Cyber Atlantic 2011 was the first joint EU-US cyber exercise and was therefore of an exploratory nature. The specific exercise objectives were:
1. Explore and improve the way in which EU Member States would engage the US during cyber crisis management activities, notably using operating procedures for cooperation during cyber crises;
2. Explore and identify issues in order to improve the way in which the US would engage the EU Member states during their cyber crisis management activities, using the appropriate US procedures;
3. Exchange good practices on the respective approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration.

The exercise was planned by a joint EU-US planners group facilitated by the European Network and Information Security Agency (ENISA) and the Department of Homeland Security (DHS).

Cyber Europe 2012

The evaluation report of Cyber Europe 2010 as well as the related policy documents (Digital Agenda, and the Commission Communication on Critical Information Infrastructure Protection, CIIP) explicitly support the scoping and organization of future pan-European exercises. Based on the above, the Member States moved forward to organise the second pan European Exercise on CIIP - Cyber Europe 2012, that took place in October 2012.

The exercise was more extensive and more sophisticated, and was based on the experience and the recommendations of Cyber Europe 2010, and learning from the Cyber Atlantic 2011 exercise. Twenty nine countries and several EU Institutions participated. The private sector actors took part in this exercise for the first time. Cyber Europe 2012 was a milestone in the efforts to strengthen cyber-

crisis cooperation, preparedness and response across Europe as stated also in the Cyber Europe 2012 - Key Findings and Recommendations report.

Other Related Activities

ENISA is presently continuing its efforts in providing support to Member States in areas such as:

- National Contingency Plans
- Organizing Pan-European and International exercises on CIIP
- Development of scenarios for national exercises Providing Seminars to Member States on how to organise and manage a national cyber exercise
- Providing Seminars to Member States on how to develop and manage a national contingency plans
- Contributes to EU efforts to develop Standard Operating Procedures for cross country cyber incidents