On National and International Cyber Security Exercises

Survey, Analysis and Recommendations

October 2012

Executive Summary

Cyber exercises are an important tool to assess the preparedness of a community against cyber crises, technology failures and critical information infrastructure incidents. ENISA supports the stakeholders involved in EU cyber exercises.

This report aims to support European and international bodies involved in cyber exercises with lessons learned about cyber exercises and recommendations for the future. The report presents the results of the ENISA 2012 research and analysis by ENISA in 2012 of national and international cyber exercises carried out.

ENISA examined 85 exercises covering the period between 2002 and 2012. In total, 84 countries worldwide participated in the multinational exercises analysed in this report. A total of 22 European countries conducted in national cyber-exercises.

The main findings in this research include:

1. The number of cyber exercises has increased in recent years (71% took place in between 2010-2012). The reasons for this increase are the overall policy context that supports and boosts cyber exercises, the increased emphasis given by the EU Member States to cyber exercises, and the increasing threat of (cross-border) cyber incidents and attacks.
2. Cyber crisis cross border cooperation efforts are continuously developing. Cyber security is an urgent matter which receives increasingly more attention in European countries.
3. Public–private partnerships during cyber exercises are essential due to private sector ownership of most critical information infrastructures. There is a need to intensify public–private cooperation in cyber exercises.
4. More attention should be paid to developing exercise management tools which can support exercise execution and preparation.
5. The use of methodological planning, monitoring and evaluation is crucial for effective exercises.
6. There is broad consensus that cyber exercises help to enhance the preparedness, responsiveness and knowledge of stakeholders in responding to cyber incidents.

The report concludes with seven recommendations for stakeholders in the global cyber exercises area, which aim to increase the number and quality of cyber exercises. The main recommendations are:

1. Establish a more integrated global cyber exercise community;
2. Ensure the exchange of good practices on cyber exercises, including public–private cooperation;
3. Support the development of exercise management tools to support exercise planning, execution and evaluation;
4. Aim for more complex cyber exercises on an inter-sectoral, international and European level;
5. Enhance preparedness by including exercises in the lifecycle of Cyber Crisis Contingency Plans;
6. Update the good practices for national exercises and initiate a good practice guide for multinational exercises;
7. Develop feedback mechanisms for ensuring that lessons learned from cyber exercises are implemented resulting in enhanced cyber crisis preparation.