enisa
European Network and Information Security Agency

Cyber Europe 2012

Key Findings and Recommendations

December 2012

Acknowledgements

ENISA wishes to thank all persons and organisations which have contributed to this exercise. In particular, our gratitude goes to the exercise planners, national monitors and moderators.

About ENISA

The European Network and Information Security Agency (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.

Follow us on Facebook Twitter LinkedIn Youtube & RSS feeds

ENISA Project Team

Panagiotis TRIMINTZIOS, ENISA
Razvan GAVRILA, ENISA
Maj Ritter Klejnstrup, ENISA

Contact details

For questions related to this report or any other general inquiries about the resilience program please use the following contact address: resilience at enisa.europa.eu

Contents

About Cyber Europe 2012

On 4 October 2012 more than 500 cyber-security professionals across Europe participated in Cyber Europe 2012, the second pan-European Cyber Exercise.

The exercise built on extensive activities at both the national and European level to improve the resilience of critical information infrastructures. As such, Cyber Europe 2012 was a milestone in the efforts to strengthen cyber-crisis cooperation, preparedness and response across Europe.

In 2009, the European Commission issued a communication on Critical Information Infrastructure Protection (CIIP): 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' (COM/2009/149). This communication gave rise to the first pan-European Cyber Exercise, which took place on 4 November 2010. The European Commission moved forward with its Digital Agenda for Europe (2010), and its 2011 communication: 'Achievements and next steps: towards global cyber-security' (COM/2011/163). Building on these efforts, Cyber Europe 2012 expanded in scope, scale and complexity.

Cyber Europe 2012 had three objectives:

1. Test the effectiveness and scalability of mechanisms, procedures and information flow for public authorities' cooperation in Europe.
2. Explore the cooperation between public and private stakeholders in Europe.
3. Identify gaps and challenges on how large-scale cyber-incidents could be handled more effectively in Europe.

Twenty-nine EU (European Union) and EFTA (European Free Trade Association) Member States were involved in the exercise; 25 of them participated actively in the exercise, while the other four were involved as observers. In addition, several EU Institutions participated. Overall, 339 organisations participated in the exercise, bringing a total of 571 individual players in action. Following up on a key recommendation of Cyber Europe 2010, the private sector actors took part in this exercise. Cooperation between public and private players took place at the national level, while public authorities also cooperated across borders. The majority of the players (88%) were positive about the exercise (see Figure 1).

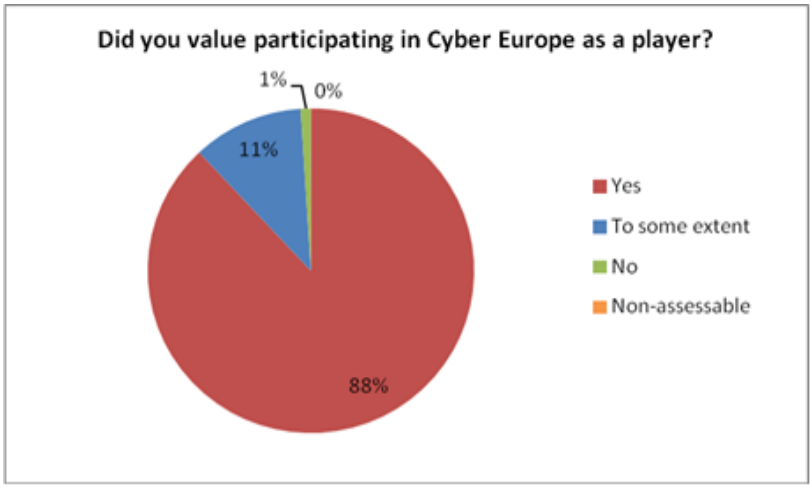


Figure 1: Level of players' satisfaction

The planning process

Cyber Europe 2012 was facilitated by the European Network and Information Security Agency (ENISA) and supported technically by the Joint Research Centre (JRC) of the European Commission. Representatives of all 25 participating countries and the European Union Institutions were involved in the planning of the exercise. The planning process was organised around several workshops.

The scenario

The exercise scenario revolved around large-scale cyber-incidents in Europe, which affected all participating countries. Fictional adversaries joined forces in a massive cyber-attack against Europe, mainly through Distributed Denial of Service (DDoS) attacks against public electronic services. The affected services were online e-government and financial (e-banking, etc.) services.

Cyber-incidents challenged the public and private sector participants, triggering a need for cross-country cooperation. Players received information on the scenario (injects) via emails, and had to collaborate using standard procedures and structures in order to assess the situation and agree upon a course of action. Figure 2 depicts the large number of email injects exchanged during the exercise.

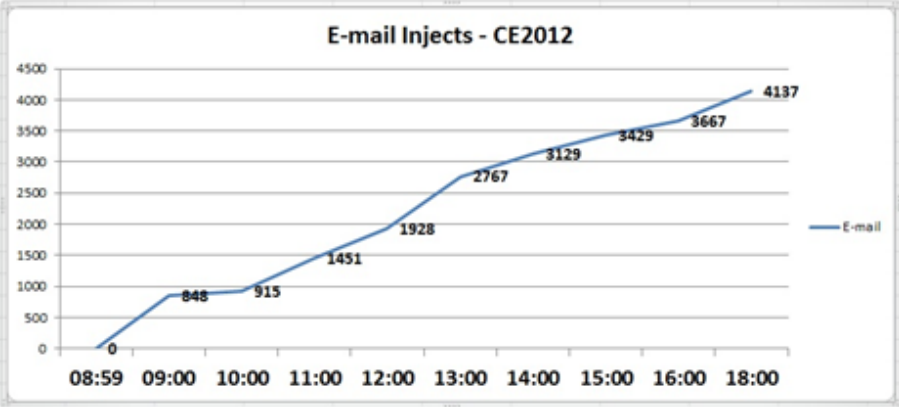


Figure 2: Email injects send out during the exercise

The Players

The exercise scenario involved many different players. Overall 571 individuals from 339 organisations around Europe took part in the exercise. There were 25 countries playing in the exercise; the European Union Institutions also played. The organisations involved were from the following groups: the cyber-security agencies and organisations, the relevant ministries, the e-government service owners, financial institutions and Internet Service Providers (ISPs) and telecommunication service operators. The distribution of players is shown in Figure 3.

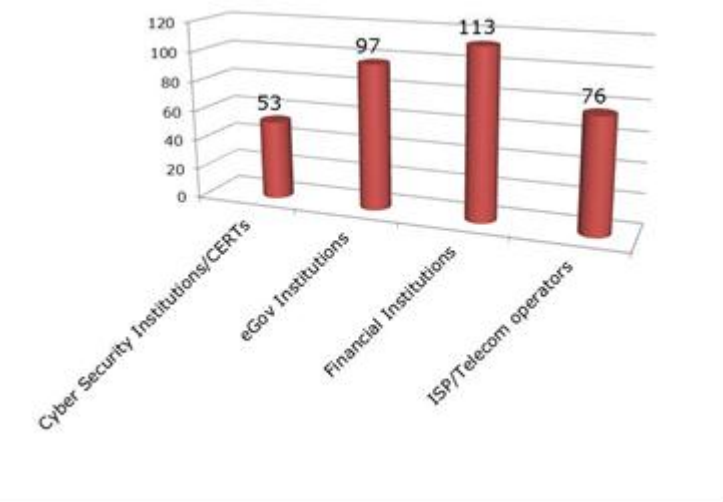


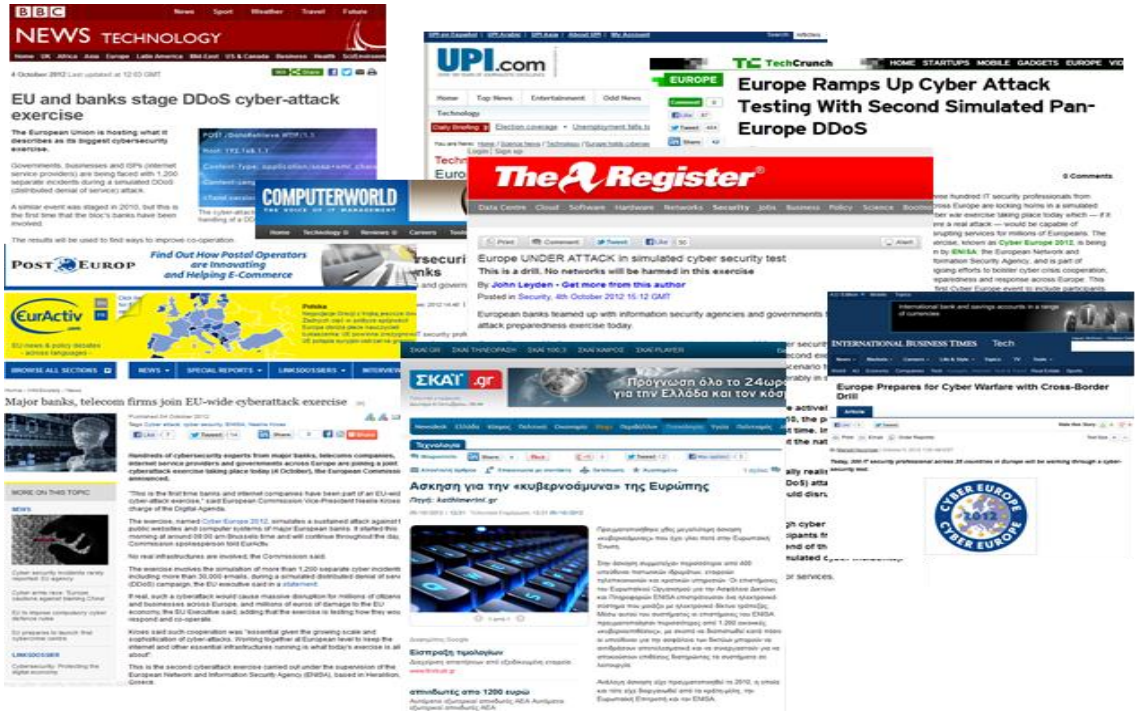
Figure 3: The distribution of the organisations that actively played in CE2012

Media attention

Cyber Europe 2012 attracted considerable attention in the global media. More than 600 articles were published in 19 languages.

Many articles quoted Vice-President of the European Commission responsible for the Digital Agenda, Neelie Kroes, stating that '*Working together at the European level to keep the Internet and other essential infrastructures running is what today's exercise is all about.*'

In addition, Cyber Europe 2012 was mentioned in social media in over six languages. The compilation of media messages in the picture below displays some of the articles published about Cyber Europe 2012.



Key Findings

Cyber Europe 2012 produced a series of key findings regarding national-level cooperation, international-level cooperation, and cyber exercises, which are summarised below:

National-level cooperation

- Playing countries, taking cyber security incidents very seriously, responded to the challenges by escalating to their national crisis response cells and/or activating national crisis structures.
- Frequent cooperation and information exchange at the national level between public and private players took place during the exercise.
- Some countries experienced challenges in crisis management decision making, even though that was not part of the exercise objectives (e.g., some of the decisions at hand have to be taken at more strategic levels during a crisis).
- Public–private cooperation structures differ from country to country. Parallel and sometimes overlapping public and private national-level procedures sometimes challenged the public–private cooperation within countries.
- The inclusion of private sector organisations as players at the national level provided an excellent improvement on the previous Cyber Europe exercise.

International-level cooperation

- Cyber Europe 2012 has proven to be an excellent opportunity to explore, understand and evaluate existing European cyber cooperation mechanisms. The exercise has strengthened the European cyber-incident management community.

- All participating countries were fully engaged in the international cooperation phase of the exercise. During the exercise many bilateral and multilateral interactions at the international level took place.
- Having a set of standard operational procedures and communication tools helped to provide structure and situational awareness during the simulated cyber-crisis.
- Challenges were identified in the operational procedures, notably in terms of scalability due to the large number of playing countries and institutions.
- Familiarity with procedures and information flows proved to be crucial for building a fast and effective response capability across Europe.
- Appropriate and up-to-date technical infrastructures and tools proved critical to ensuring effective cooperation.
- Cyber Europe 2012 helped to build trust between countries, which is key to successful and timely mitigation activities during real cyber-crises. The exercise has fostered both new and existing relationships.

Cyber exercises

- The European cyber-incident management community considers pan-European exercises as an important tool for evaluating and improving existing cyber-crisis cooperation frameworks.
- Cyber Europe 2012 has proven extremely useful for testing national contingency measures and levels of preparedness.
- Cyber exercises are very useful to build trust among different cyber communities.
- Efficient planning is crucial for conducting an effective, large-scale, and complex exercise.

Recommendations

Cyber Europe 2012 resulted in the following recommendations:

- Cyber Europe 2012 proved valuable in enhancing pan-European cyber-incident management. It is therefore important to continue the efforts and further develop the European cyber exercise area. EU Member States and EFTA countries should cooperate towards new pan-European and national cyber exercises in order to enhance transnational cyber-incident management. The Good Practice Guide on National Exercises[1], developed by ENISA, provides additional support in this area.
- Future cyber exercises should explore inter-sectoral dependencies and be more focused on specific communities.
- Cyber Europe 2012 provided an opportunity for international-level cooperation and strengthening of the European cyber-incident management community. To foster international cooperation it is essential to facilitate exchange of good practices in cyber

[1] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises

exercises, lessons learned, expertise and the organisation of conferences. This will ensure a stronger community that is able to tackle transnational cyber-crises.

- EU Member States and EFTA countries should further improve the effectiveness, scalability of, and familiarity with, existing mechanisms, procedures and information flows for cooperation at national level and with other public authorities in Europe. Lessons learned from Cyber Europe 2012 provide an excellent starting point.
- All stakeholders in the area of international cyber-crisis cooperation need to be trained on the use of procedures in order to know how to adequately work with them.
- The involvement of private sector organisations as players was of added value to this exercise. Therefore, EU Member States and EFTA countries should consider the involvement of the private sector in future exercises.
- The European cyber-incident management community could be strengthened with input from other European critical sectors (e.g. health, transportation) that are relevant to the handling of large-scale crises.

Further information on cyber-crisis cooperation and exercises can be found at ENISA's web pages at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation

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