European Union Agency for Network and Information Security

ENISA CE2014

After Action Report

Public version

enisa.europa.eu

Report on Cyber Crisis Cooperation and Management

Authors

ENISA Cyber Crisis Cooperation and Exercises (C3E) program team:

Razvan Gavrila, Adrien Ogée, Panagiotis Trimintzios (Program Manager) and Alexandros Zacharis.

Acknowledgements

ENISA would like to thank to all participants in Cyber Europe 2014 for their valuable contribution.

Contact

Cyber Crisis Cooperation team: c3@enisa.europa.eu

Disclaimer

A full version of the After Action Report, containing detailed observations, challenges, recommendations and actions has been made available to all national cybersecurity authorities which participated in Cyber Europe 2014. All participants to the exercise interested in the full version shall liaise with their national cybersecurity authority.

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 MS, 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 MS 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 MS 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 http://www.enisa.europa.eu.

Follow ENISA on

Facebook Twitter LinkedIn YouTube and RSS feeds

Contact details

For contacting ENISA or for general enquiries on Privacy please use the following details:

Email: sta@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2015

Reproduction is authorised provided the source is acknowledged.

ISBN: 978-92-9204-128-1 DOI: 10.2824/123012 Catalogue number: TP-04-15-624-EN-N

Executive Summary

Cyber Europe offers to 32 different countries, Member States of the European Union (EU) and the European Free Trade Association, hereafter collectively referred to as the Member States (MS), the possibility to engage in cooperation activities at various levels with the shared objective to mitigate jointly large-scale cybersecurity incidents. The EU Standard Operational Procedures (EU-SOPs), used to support these cooperation activities, provide Member States with guidelines which they can use in the face of large-scale cybersecurity incidents.

The main goal of Cyber Europe 2014 was to train Member States to cooperate during a cyber crisis . The exercise also aimed at providing an opportunity to Member States to test national capabilities, including the level of cybersecurity expertise and national contingency plans, involving both public and private sector organisations. In order to address the different layers of cyber crisis management, Cyber Europe 2014 was divided in three escalating phases, spread over 2014 and early 2015.

The exercise was a success, for it allowed ENISA to draw numerous lessons, recommendations and concrete actions, which will help to enhance cyber crisis preparedness in Europe. The common ability to mitigate large scale cybersecurity incidents in Europe has progressed significantly since 2010 when the first Cyber Europe exercise was organised. In particular, Cyber Europe 2014 has shown how valuable it is to share information from many different countries in real-time in order to facilitate high-level situation awareness and swift decision-making. Nevertheless, such processes are unprecedented in real-life and hence requires primarily capability development and possibly also policy guidance from both the Member States as well as the EU Institutions and Agencies.

It is crucial that Member States continue to rely upon and improve multilateral cooperation mechanisms, which complement the bilateral and regional relations they have with trusted partners. The EU-SOPs, which are meant to support the former, will be further improved to better take into account the evolving cybersecurity policy context in Europe. In addition, experience gathered throughout this exercise and the previous ones will strongly guide the development of future EU cyber cooperation instruments and exercises.

The full after action report includes an engaging action plan which ENISA and Member States are committed to implement.

[1] For more information on cyber crises, please refer to the ENISA Report on Cyber Crisis Cooperation and Management: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study

Contents

1. Exercise overview

1.1 Objectives and setup

The goal of this exercise has been to contribute to the training of Member States' participating organisations with a view to help them cooperate during a cyber crisis. More specifically, this exercise provided opportunities to assess the effectiveness of cooperation and escalation procedures in the face of cross-border cyber incidents which impact the security of vital services and infrastructure.

CE2014 had the following key objectives:

1. Test the European alerting, cooperation and information exchange procedures between national-level authorities responsible for cyber incidents.
2. Provide an opportunity for Member States to test internally their national NIS contingency plans and capabilities.
3. Explore the effect of multiple and parallel information exchanges between private-public and private-private.
4. Explore the NIS incident response escalation and de-escalation processes (technical-operational-political).
5. Explore the public affairs handling of large-scale cyber incidents.

In order to better tackle the challenges of each layer involved in crisis management, the exercise was divided into three phases: technical, operational and strategic, each phase escalating into the next one.

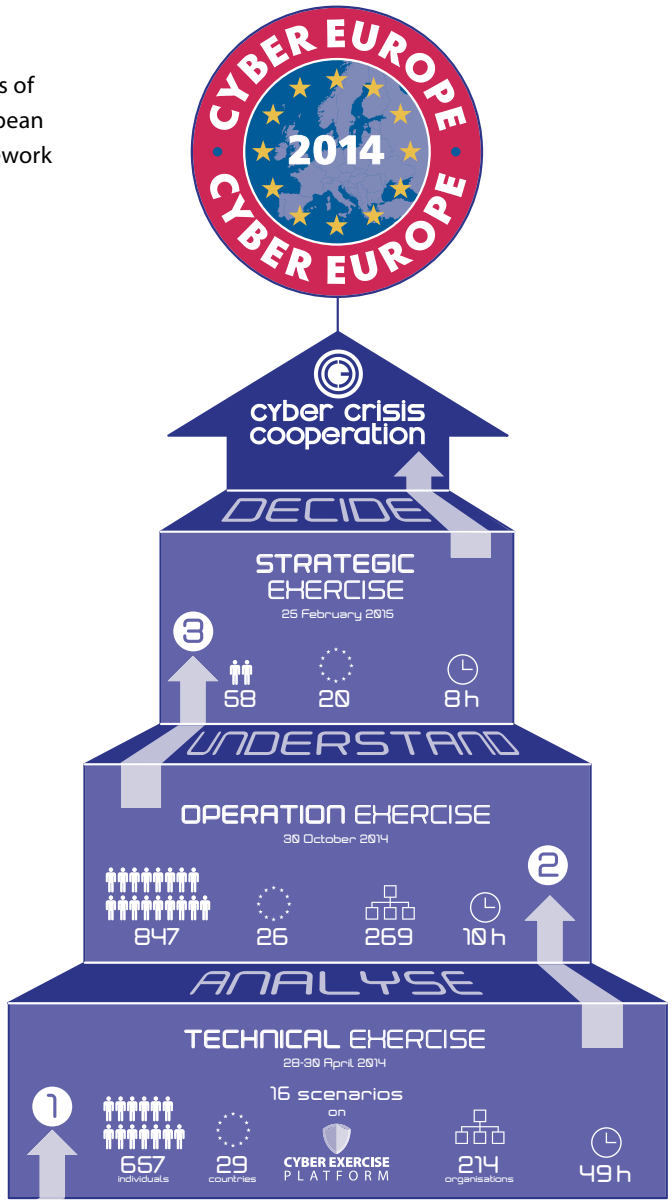


Figure 1: Mapping of the phases of Cyber Europe 2014 to the European Cyber Crisis Cooperation Framework (ECCCF) Model.

1.2 Planning

The exercise was organised by ENISA and planned jointly with representatives from the participating Member States. It required six planning conferences which took place in Belgium, Greece (twice), Luxembourg, Netherlands and Spain.

1.3 Exercise platform

The exercise planning, conduct and evaluation was supported by the ENISA Cyber Exercise Platform (CEP). Developed by ENISA, CEP allows to:

- Work on all planning documentation (including Exercise Plan, Scenarios, Incidents/Injects, Policies, Press Releases, etc.).
- Facilitate the exercise communication.
- Support the development of incidents and injects.
- Conduct the exercise (send injects, monitor progress, reporting, etc.).
- Simulate the exercise world (news and media, social media, videos, etc.).
- Evaluate the exercise (polls, surveys, after action report production).
- Stay up-to-date with the exercise events and logistics.

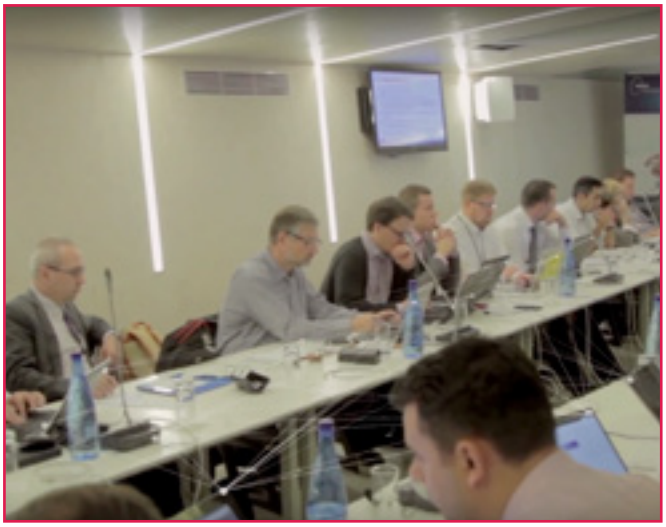
CEP is currently being further developed by ENISA in order to be leveraged in future cyber exercises. ENISA accepts requests to contribute to future developments of the platform. In case of interest, please contact the ENISA Cyber Crisis Cooperation team (c3e@enisa.europa.eu). Any requests received will be evaluated and requesting parties will be informed accordingly of their expected contribution and role as appropriate.

CYBER EXERCISE
PLATFORM

2. Participation

The recruitment of participants was the responsibility of the exercise planners (one per Member State and Institution).

Participation	Nb
Countries	29
Organisations	214
Individuals	657
Cybersecurity agencies	23
CSIRTs	48
Other Public Sector Institutions	50
Energy sector	27
Telecom sector	25
ICT Vendors	22
Financial sector	8
EU institutions	11



2.1 Technical level exercise (TLEx)

Participants of TLEx came from 29 countries and the EU Institutions. The participatin teams were composed of technical experts from public and private CERTs.

2.2 Operational level exercise (OLEx)

Participants to OLEx were operational crisis management teams from cybersecurity agencies, national and/or governmental CERTs, as well as crisis management teams from private companies in the telecom and energy sectors.

Participation	Nb
Countries	26
Organisations	269
Individuals	841
Public sector (expert: cybersecurity agencies, national and governmental CERTs)	121
Public sector (non-expert: ministries, etc.)	61
Private sector: telecom	41
Private sector: energy	50

2.3 Strategic level (SLEx)

Participants to SLEx were senior officials responsible for the management of the cybersecurity components of a crisis within the relevant national authorities.

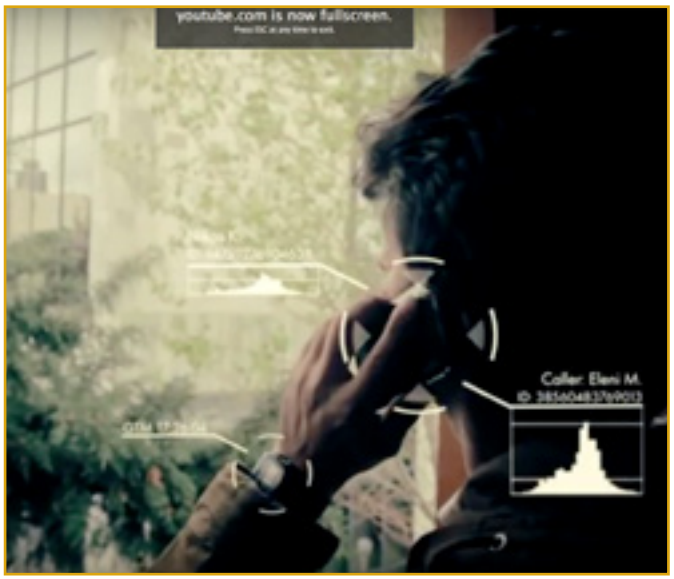
Participation	Nb
Countries	20
Individuals (public sector)	58

3. Scenario overview

The scenario of Cyber Europe 2014 revolved around a proposal for an EU regulation related to Member States' importing of energy resources. The regulation aimed to introduce a tax to fund the development of green technologies such as wind farms, solar roads and electric cars. Opponents to the regulation claimed its objective was merely to increase taxes in the midst of the economic crisis. Several countries around the world, potentially impacted by such regulation, claimed that it was a geopolitical manoeuver aimed at undermining their development. Large lobbying and disinformation campaigns were organised to influence the decision on the EU regulation. Despite these efforts, negotiations moved forward and Member States and EU Institutions became the target of cyber attacks aimed at exfiltrating information about the regulation and destabilizing its energy market. The technical phase (TLEx) of Cyber Europe 2014 was organised at this point in the scenario, with incidents ranging from open source intelligence gathering on social media, mobile phone malware analysis to denial of service attacks and advanced persistent threats.

The disruptions caused by these attacks did not prevent the regulation from passing. This led to a series of large-scale cyber attacks, with the goal to instigate fear and prevent the voting of the regulation. Several 0-day vulnerabilities were used to develop advanced exploits, attack various critical infrastructure operators' networks and numerous online services. The operational phase of Cyber Europe 2014 (OLEx) was organised at this point in the scenario.

The crisis then escalated further, with several energy infrastructure operators severely impacted in the midst of a harsh winter, key critical technologies breached and an increasingly worried public opinion. The strategic phase of Cyber Europe 2014 (SLEx) was organised at this point in the scenario.



4. Key findings and recommendations

The key findings from Cyber Europe 2014 are the following:

- Cyber Europe 2014 proved to be an excellent opportunity to explore, understand and evaluate existing European cyber cooperation mechanisms at the technical, operational and strategic levels. The exercise strengthened the European cybersecurity community.
- Participants were fully engaged in cooperation at national and European levels, which led to a shared understanding of all facets of the crisis within a few hours.
- During the exercise, many multilateral interactions at the international level took place, highlighting the importance of regional cooperation.
- The EU Standard Operational Procedures and communication tools helped to provide higher situational awareness and structured cooperation activities during the simulated cyber crisis.
- Increased familiarity with these procedures could allow for a faster response.
- The large majority of participants recognised the benefits of exercising for the first time a strategic-level cooperation.
- Cyber Europe 2014 contributed to trust building between Member States as it fostered new relationships and strengthened existing ones.
- The participating organisations took the scenario seriously and responded adequately to all challenges, either mitigating incidents at the technical level or using their respective contingency and business continuity plans.
- Participants to the technical phase recognised that it refreshed, if not increased their cybersecurity capabilities: 98% indicated interest to participate in the next exercise.
- The Cyber Exercise Platform proved to be a powerful tool to plan, conduct and evaluate the exercise.
- The introduction for the first time of the three phases in Cyber Europe was an important step towards understanding the inner challenges of such large scale crisis management processes.
- Large scale cyber exercises such as Cyber Europe 2014 are complex projects which require a long planning phase (over 2 years) and the contribution of scarce expertise, both from ENISA and the Member States.

5. key recommendations from the exercise

The following are the key recommendations from the exercise:

1. Cyber Europe exercises, as well as any cooperation activity at European level during real cyber crises, build upon existing relations between Member States. ENISA and the Member States will continue to invest in trust building activities to maintain and further develop existing trust.
2. ENISA and the Member States should further develop the operational procedures which drive the cooperation activities during a cyber crisis, taking into account existing and future cooperation frameworks, to bring these procedures to a maturity level similar to those found in other sectors such as civil protection and aviation.
3. ENISA and the Member States will seek further integration with national and regional activities.
4. ENISA will address future Cyber Europe activities as a programme containing both trainings as well as small and large scale exercises, in order to provide a better experience and achieve greater impact.
5. Lastly, ENISA will further develop the Cyber Exercise Platform to offer a richer experience to both players and planners, as well as to support the organisation of national and regional exercises, fostering the development of a cyber exercise community.

European Union Agency for Network and Information Security

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 Vasilissis Sofias Str.
ENISA building
Marousi 151 24, Athens, Greece

enisa.europa.eu

Catalogue Number: TP-04-15-624-EN-N