enisa

THE EU CYBER SECURITY AGENCY

CYBER EUROPE 2016: AFTER ACTION REPORT

Findings from a cyber crisis exercise in Europe

JUNE 2017

CONTACT

For queries in relation to this paper, please email: c3@enisa.europa.eu
For media enquiries about this paper, please email: press@enisa.europa.eu

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, 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 the current state of affairs 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

Catalogue number: TP-01-17-327-EN-N
ISBN: 978-92-9204-224-0
DOI: 10.2824/218244

CYBER EUROPE 2016: AFTER ACTION REPORT

Findings from a cyber crisis exercise in Europe

TABLE OF CONTENTS

SECTION I

EXECUTIVE SUMMARY

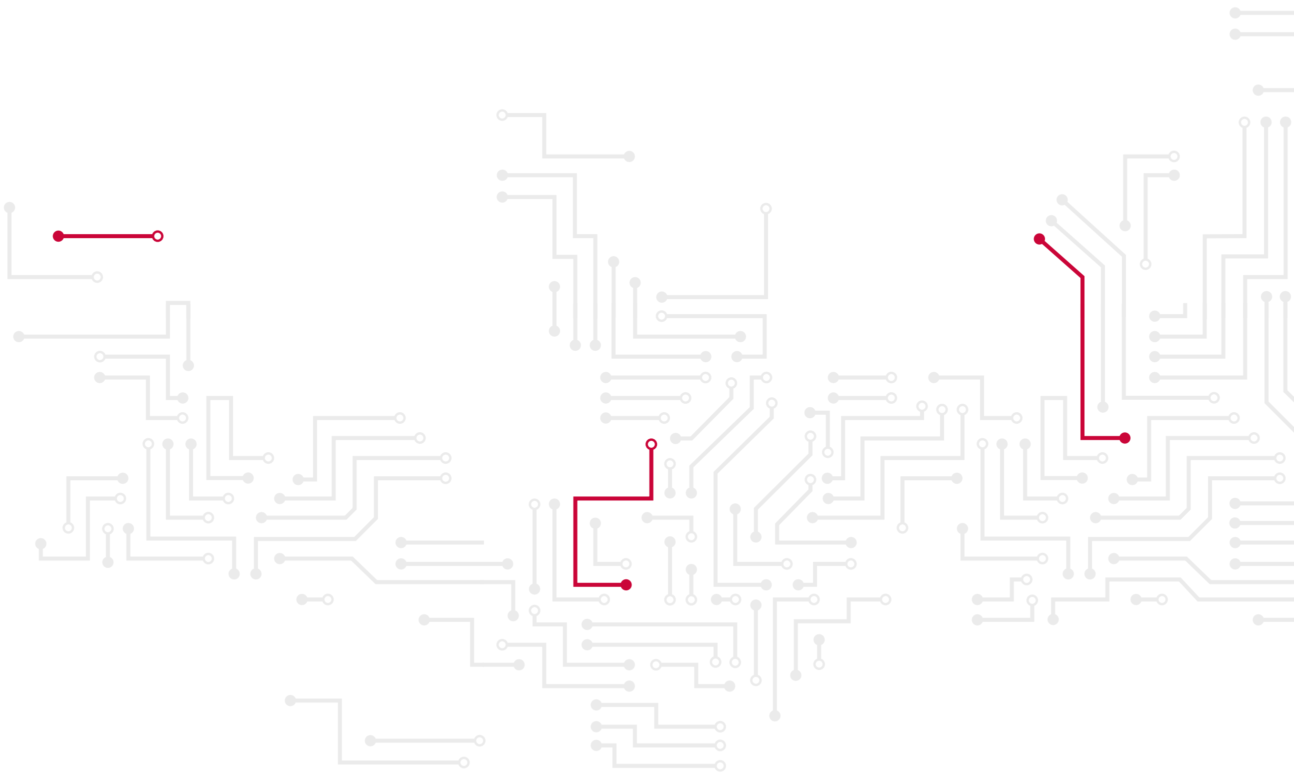
Cyber Europe 2016 was the fourth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA). Over 1 000 participants working mostly in the ICT sector, from public and private organisations from all 28 Member States of the European Union and two from the European Free Trade Association (EFTA), joined in a programme of activities ranging from training sessions and communication checks to technical competitions and cooperation exercises.

The exercise simulated a realistic crisis build-up over an actual period of 6 months, culminating in a 48 hour event on 13 and 14 October 2016.

Cyber Europe 2016 was based on three pillars essential to the successful mitigation of large-scale crises caused by cybersecurity incidents: cooperation at national and international levels and sound cybersecurity capabilities.

First, the exercise fostered cooperation between targets of simulated cybersecurity incidents, security providers and national authorities, shedding light on national-level public–private and private–private cooperation. Participants had to follow existing business processes, agreements, communication protocols and regulations to mitigate effectively the situations presented to them. Such mechanisms were not always in place for all participants, which hindered the overall ability to reach full EU-level situational awareness. The EU network and information security directive identifies many of the associated shortcomings and proposes measures that ENISA and Member States are already implementing to improve the situation.

Second, Cyber Europe 2016 helped participants understand how cybersecurity authorities would cooperate with each other and EU bodies in the event of a large-scale crisis. Undoubtedly, crisis cooperation at EU level is very much maturing and improving. Most, if not all, Member States have come to realise the importance of sharing structured information across national borders. With the active support of ENISA, they have leveraged the benefits of EU-level situational awareness for their own crisis management activities. Yet despite such progress, Cyber Europe 2016 highlighted, as previous exercises did, the absence of a cooperation framework at EU level for crises stemming from cybersecurity incidents, officially endorsed cooperation procedures or a centralised



hub. The creation of the EU CSIRTs Network and the European Commission initiative to publish a crisis cooperation blueprint in 2017 are excellent developments in that regard. They will surely benefit from the detailed findings in this report.

Last, the exercise offered countless opportunities for participants to enhance their cybersecurity capabilities, from their technical and operational expertise to their capacity to handle crisis communication. Organisational and individual cybersecurity preparedness and capabilities in the EU were excellent overall. Technical expertise, business continuity and crisis communications procedures were of a high standard. Nevertheless, the vision required to link technical- and operational-level response activities to strategic crisis management mechanisms was sometimes lacking, which proved detrimental to fostering crisis exit strategies supporting decision-making.

Additionally, many lessons were learned from the use of the prototype platforms developed by ENISA to support cooperation at EU level; they will reflect positively on the development of the EU-level crisis cooperation infrastructure financed by the Connecting Europe Facility (CEF).

KEY FINDINGS AND RECOMMENDATIONS

KEY FINDINGS

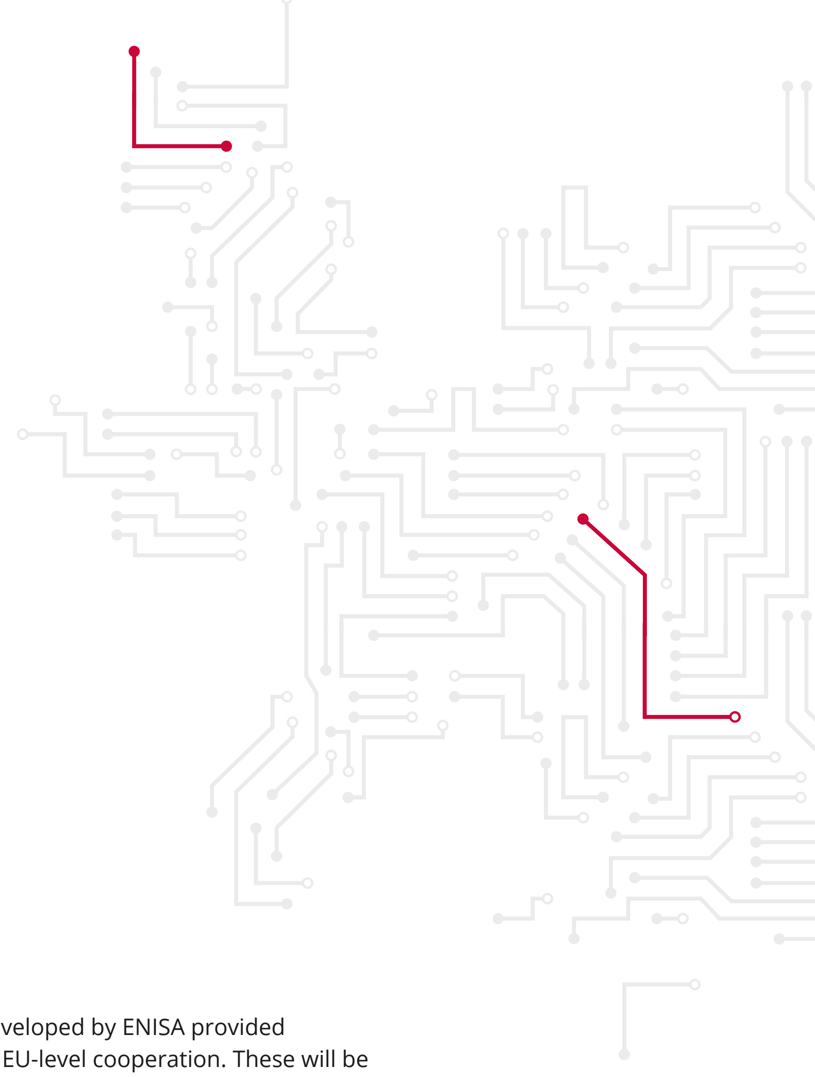
Participating organisations responded adequately to most challenges they faced during the exercise. Cybersecurity experts employed in a wide array of sectors in the EU demonstrated high levels of expertise and appetite to resolve complex cybersecurity issues. Their ability to cooperate in the most difficult times is an important finding.

No participant questioned the essence of cyber incident cooperation at EU level. Rather, all actors focussed their efforts on lifting the remaining barriers. Such cooperation was particularly insightful and led to a full understanding of all facets of the crisis within a few hours, which supported the swift mitigation of a simulated large-scale attack against EU interests. In particular, the EU Cyber Standard Operational Procedures helped to provide EU-level situational awareness and structured cooperation activities.

The exercise in itself proved to be an excellent opportunity to increase individual and collective knowledge in the field of cybersecurity. Participants developed skills, procedures and relationships. Most importantly, they reiterated their appreciation in the exercise series: 99% indicated interest to participate in the next exercise.

Innovation and transformation were at the heart of Cyber Europe 2016. From a product, process, rhetoric and service perspectives, the exercise planning team, composed of Member States and ENISA representatives, pushed established boundaries to transform the EU cybersecurity society. The European Union Ombudsman underlined this joint effort in March 2017 with an award for excellence in innovation and transformation.

Participants repeatedly asked for more opportunities to test their technical skills regularly against a variety of advanced scenarios. Many were grateful for the multiple options offered by ENISA to involve media, legal and financial policy experts and hope for more to come as leaders across the EU realise that cybersecurity goes beyond information security.



The Cyber Crisis Cooperation Platform prototype developed by ENISA provided numerous insights into technical means supporting EU-level cooperation. These will be of paramount importance in order to ensure the buy-in from Member States in such a cooperation platform, currently under development.

The Cyber Exercise Platform proved to be a powerful tool to plan, conduct and evaluate the exercise. In particular, the simulated environment developed by ENISA supported the crisis build-up in a realistic fashion with an unprecedented emphasis on written and visual storytelling.

Key recommendations

1. Following their revision, the operational procedures which drive the cooperation activities during a cyber crisis should be endorsed by the CSIRTs Network established by the Network and Information Security Directive. Training opportunities on the use of these procedures and tailored exercises should be offered regularly.

2. An EU-level cyber crisis cooperation framework is currently being developed by the European Commission. It should build upon these findings to develop interconnections between cooperation mechanisms, identify and empower key actors, from CSIRTs to law enforcement, and set a clear vision for the future of EU cyber response.

3. Future Cyber Europe should focus on cooperation activities on technical and operational topics. Other options should be pursued to offer training and exercise opportunities on a variety of other topics increasingly associated with cybersecurity. In particular, ENISA should support EU-wide capacity building on cyber crisis communication.

SECTION I
EXERCISE OVERVIEW

1.1 GOALS AND OBJECTIVES

The three goals of the Cyber Europe 2016 exercise built upon those set in Cyber Europe 2014, following an in-depth assessment of their relevance performed in the after action report of the latter exercise[1].

G1. Test EU-level cooperation processes.

G2. Provide opportunities for Member States to test their national-level cooperation processes.

G3. Train EU- and national-level capabilities.

Consequent objectives were derived from the high-level goals in order to drive the development of the exercise, as presented in Table 1 (next page).

1.2 TARGET AUDIENCE

Participation in Cyber Europe 2016 was limited to organisations from the European Union institutions, European Member States and European Free Trade Association Member States (collectively called Member States hereafter), and private companies operating in the latter countries.

The main target audience of the exercise was individuals and organisations involved in information security activities in the information and telecommunications technology (ICT) sector.

Some Member States chose to involve individuals and organisations from other sectors as well, as indicated in Figure 1.

In total, 948 participants officially registered for the exercise, of whom two thirds came from the private sector.

NB: These figures account only for those participants who registered in the Cyber Exercise Platform. Several organisations chose to use one account and distribute exercise information between multiple participants. As a result, one can assume the actual total number of participants to be significantly higher.

1.3 SET-UP

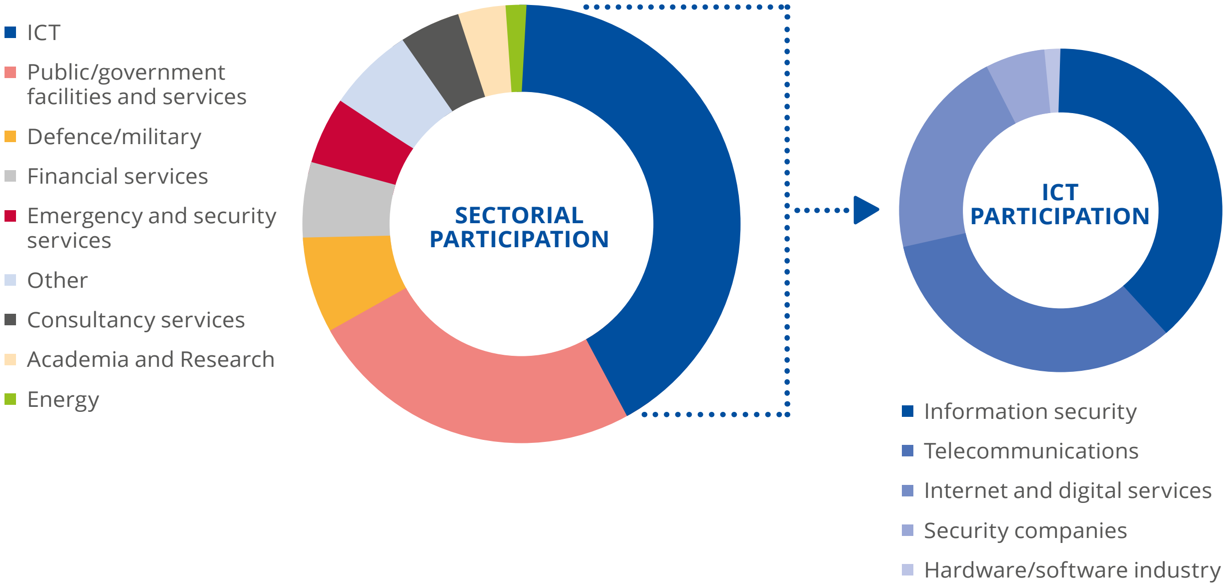
Cyber Europe 2010 and 2012 were 1-day all-inclusive exercises. Cyber Europe 2014 was the first exercise in the series in which technical cybersecurity incident handling was combined with operational crisis management activities in three different phases. Building upon the latter, Cyber Europe 2016 was a collection of exercising activities, offering prolonged opportunities to participants to learn, train and exercise their technical and operational capabilities.

[1] https://www.enisa.europa.eu/publications/ce2014-after-action-report

Table 1 — Goals and objectives

STRATEGIC GOAL	OBJECTIVE	METRICS/QUALITATIVE INDICATORS
G1	**O1.** Assess the quality of information sharing	Timeliness, usefulness, structured vs unstructured
	O2. Monitor occurrences of cooperation activities	Number of EU CSOPs cooperation activities held, e.g. meetings/audioconferences, during the exercise
	O3. Evaluate situational awareness	Completeness, timeliness, usefulness of EU cyber integrated situation report
	O4. Assess the ability to develop exit strategies	Appropriateness and usefulness of the proposed actions
G2	**O5.** Provide opportunities to participants to test their intra-organisational procedures, if they exist (BCPs, crisis management plans, etc.)	Number of opportunities provided to and used by participants
	O6. Provide opportunities to participants to test cross-organisational cooperation processes, if any	Number of opportunities provided to and used by participants
	O7. Provide opportunities to participants to test national-level cooperation activities and/or contingency plans, if they exist	Number of opportunities provided to and used by participants
G3	**O8.** Provide opportunities to train a wide variety of cybersecurity-related skills	Number of different types of training opportunities offered, number of participants who used the training opportunities, level of satisfaction of participants in training opportunities
	O9. Provide learning opportunities	Number of learning opportunities offered to participants
	O10. Provide self-assessment opportunities	Types of self-assessment opportunities offered to and used by participants
	O11. Identify training needs for the future	Number of different types of training needs identified

Figure 1 — Participation



[2] https://www.enisa.europa.eu/publications/ce2014-after-action-report

The Cyber Europe 2016 programme was comprised of activities in three areas.

1. Training sessions (from September 2015 to October 2016)

- On-site training on exercise planning provided during the initial and main planning conferences.
- On-site crisis planning and management training for public participants.
- Online training on the EU cyber standard operational procedures (EU-CSOPs) and the pilot cooperation platform offered to representatives of EU national and governmental computer security incident response teams (CSIRTs).

2. Preparatory exercises (from April to October 2016)

- Technical cybersecurity challenges released every month between April and October 2016, all part of the overall Cyber Europe 2016 scenario, building up into a crisis in a realistic fashion over the course of 6 months.
- EuroSOPex, an exercise organised in June 2016 involving 24 countries split into four separate groups. This exercise helped to train the representatives of the EU national and governmental CSIRTs on the use of the EU-CSOPs.

3. Main exercise (13–14 October 2016)

An all-inclusive cybersecurity exercise building upon:

- technical cybersecurity incident analysis;
- business continuity and crisis management, including media pressure handling;
- intra- and inter-organisational cooperation at national and international levels;
- escalation;
- situational awareness.

1.4 SCENARIO

In the midst of the finalisation of the NIS directive[3], physical sabotage attempts via cyber means and attacks against the digital market, the following narrative ark was used as a driver for the development of the scenario material:

The European ICT industry is one of the most advanced in the world. Making the EU's single market fit for the digital age could contribute EUR 415 billion per year to our economy and create hundreds of thousands of new jobs. The pervasiveness of high-speed connectivity and the richness and quality of online services in the European Union are among the best globally. Such advantages have considerably increased the dependability of EU citizens on ICT services. These two elements — quality of services and customer base — make this industry particularly appealing to global business. What if this important piece of the global economy becomes a target? Computer security attacks are increasingly used to perform industrial reconnaissance, lead disinformation campaigns, manipulate stock markets, leak sensitive information, tamper with customer data and sabotage critical infrastructures.

The detailed scenario of the exercise consisted of hundreds of documents including:

- structured and unstructured, useful and misleading data scattered in simulated online blogs, magazines, forums and file storage infrastructure;
- thousands of simulated personal and professional social media profiles on simulated platforms;
- a simulated news channel, depicting the event through filmed news reports in a realistic fashion, supported by simulated formal written news websites containing hundreds of news articles;
- hundreds of tailor-made documents supporting the scenario for participants to analyse, from technical incident material to legal and public affairs documents.

1.5 PLANNING

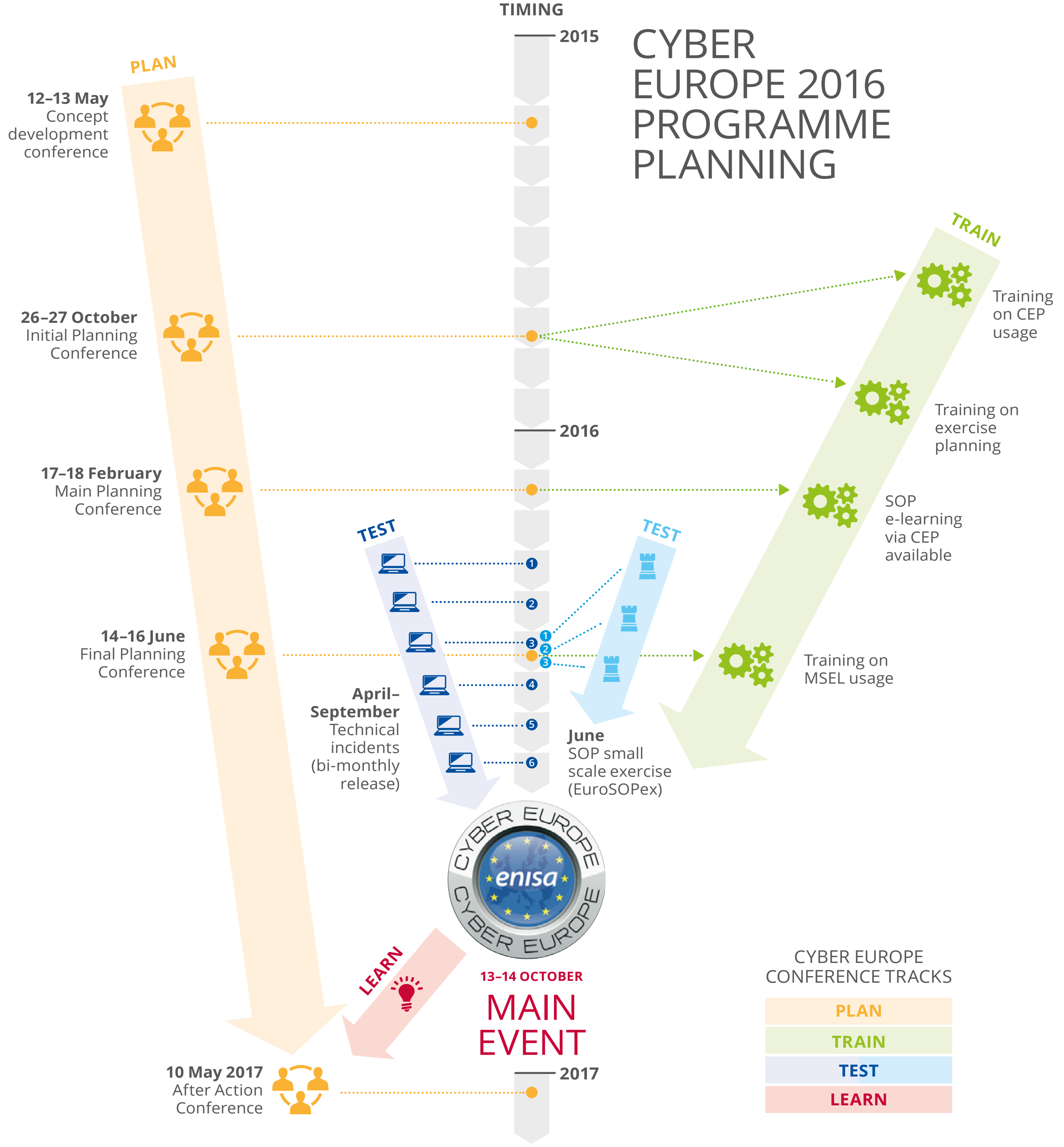
Key dates of exercise programme planning and delivery of activities were:

- 12–13 May 2015: concept development conference — Rome;
- 26–27 October 2015: initial planning conference — Athens;
- 17–18 February 2016: main planning conference — Lisbon;
- late May-early June 2016: EuroSOPex exercise;
- 13–17 June 2016: final planning conference — Athens;
- April-Oct 2016: pre-exercise release of technical challenges;
- 14–15 September 2016: dry run — Athens;
- 13–14 October 2016: main exercise event — distributed/exercise control in Athens.

[3] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

A graphical timeline of the Cyber Europe 2016 programme planning process and the programme activities is shown in Figure 2.

Figure 2


TIMING
2015
2016
2017
CYBER EUROPE 2016 PROGRAMME PLANNING
PLAN
12–13 May
Concept development conference
26–27 October
Initial Planning Conference
17–18 February
Main Planning Conference
14–16 June
Final Planning Conference
10 May 2017
After Action Conference
TRAIN
Training on CEP usage
Training on exercise planning
SOP e-learning via CEP available
Training on MSEL usage
TEST
1
2
3
4
5
6
April–September
Technical incidents (bi-monthly release)
TEST
1
2
3
June
SOP small scale exercise (EuroSOPex)
CYBER EUROPE
enisa
CYBER EUROPE
LEARN
13–14 OCTOBER
MAIN EVENT
CYBER EUROPE CONFERENCE TRACKS
PLAN
TRAIN
TEST
LEARN

A graphical timeline of the Cyber Europe 2016 programme planning process and the programme activities is shown in Figure 2.

1.6 EVALUATION PROCESS

In order to evaluate the exercise against the objectives and key performance indicators presented in Section 1.1, ENISA collected feedback from participants to the various activities of the Cyber Europe 2016 programme, as well as statistics from the different exercise platforms.

Technical cybersecurity challenges

- Anonymised statistics about incident results (see Annex 2).
- Incident-specific feedback forms.

EuroSOPex

- Evaluation survey results (see Annex 1).
- Platform and chat logs.
- National and EU integrated situation reports.
- Audioconference minutes.

Main event

- Evaluation survey results (see Annex 3).
- Observation and status reports.
- Platform logs.
- National and EU integrated situation reports.
- Audioconference minutes.

Observations, challenges, recommendations and actions drawn from the analysis of the findings highlighted in the elements mentioned above, are analysed as follows:

- Chapter 2: findings related to EU-level cooperation;
- Chapter 3: findings related to national-level cooperation;
- Chapter 4: findings related to training at national and EU levels;
- Chapter 5: findings related to exercise organisation.

An action plan summary and four annexes containing detailed results complement the report.

Given the sensitivity of some of the lessons learned, three versions of this report exist:

- a full version, available only to EU national and governmental CSIRTs (TLP AMBER) and Member States' exercise planners;
- a version without the findings related to EU-level cooperation, available to all participants in Cyber Europe 2016 (TLP GREEN);
- a public version (TLP WHITE), containing only Chapter 1.

NB: ENISA consulted planners from the respective participating Member States upon drafting this report and integrated consensual feedback. Non-consensual feedback was added to Annex 5.

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.

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
151 24 Marousi, Attiki, Greece

Catalogue number: TP-01-17-327-EN-N
ISBN: 978-92-9204-224-0
DOI: 10.2824/218244

enisa.europa.eu