THE EU CYBERSECURITY AGENCY

CYBER EUROPE 2018: AFTER ACTION REPORT

Findings from a cyber crisis exercise in Europe

DECEMBER 2018

CONTACT

For queries in relation to this paper, please email exercises@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 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-06-18-410-EN-N
ISBN: 978-92-9204-287-5
DOI: 10.2824/369640

enisa

CYBER EUROPE 2018: AFTER ACTION REPORT

Findings from a cyber crisis exercise in Europe

EUROPEAN UNION AGENCY FOR
NETWORK AND INFORMATION SECURITY

TABLE OF CONTENTS

Executive summary 6

Key findings and recommendations 7

PART I

EXERCISE OVERVIEW 9

1.1 GOALS AND OBJECTIVES 9

1.2 TARGET AUDIENCE AND PARTICIPATION 9

1.3 PLANNING AND SET-UP 11

1.4 SCENARIO 12

1.5 EVALUATION 12

1.6 KEY RECOMMENDATIONS 13

EXECUTIVE SUMMARY

Cyber Europe 2018 was the fifth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA). The exercise engaged around **900 participants**, from the public authorities and private companies, mainly in the Aviation sector, from all **28 EU Member States** as well as **two European Free Trade Association (EFTA) countries**, Norway and Switzerland.

The exercise simulated an intense realistic crisis caused by a large-number (**over 600 hundred**) of **cybersecurity incidents** that occurred during the two-days, 6-7 June 2018. The exercise was built on three main pillars:

- The sound use of business continuity and crisis management plans within an organisation
- National-level cooperation and use of contingency plans
- Cross-country cooperation and information exchange

In addition, the exercise gave the opportunity to the technical teams to **test their skills in cybersecurity** with a vast variety of technical challenges, including malware analysis, forensics, mobile malware, APT attacks, network attacks, IoT device infection, etc.

The exercise brought up the **importance of cooperation** between the different actors (victims and authorities) of simulated cybersecurity incidents, security providers and national authorities. It proved to the participants that only by **information exchange and collaboration**, it is possible to respond to such extreme situations with a large number of simultaneous incidents. We have witnessed a large number of instances of **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. Nevertheless, the level of preparedness varied significantly between participants, the **information flow** felt sometimes to be **unidirectional** and structured private-public cooperation procedures were immature or non-existent. The EU Network and Information Security (NIS) directive identifies many of the associated shortcomings and proposes measures to improve the situation.

The **EU-level cooperation has been undoubtedly improved** over the last years. In particular, the **technical-level cooperation** has proven **mature** and **effective**. The introduction of the **CSIRTs Network (CNW)** as defined in the NIS directive has provided EU Member States with an effective formal structure to exchange technical information but also to collaborate in order to resolve complex, large-scale incidents. The exercise proved that at this level EU is well equipped to respond. Some **minor gaps were identified** and have been already tackled by those involved. On the other hand, the operational-level cooperation was exercised to a lesser extent. It is not so obvious how in real-life these levels will interact and furthermore how they will implement the strategic vision of the political leaders. Future exercises shall try to test these aspects as well.

Finally, the technical incidents of the exercise provided an excellent opportunity for the cybersecurity teams to enhance their capabilities and expertise to deal with a variety of cybersecurity challenges. The **operational capacity** as well as the **technical skills** in all participating organisation proved to be at the **highest level**. Participating teams from non-cybersecurity private companies in the Aviation sector analysed the majority of incidents successfully, and proved that their skillset in certainly very high. The only shortcoming in some cases was not the lack of skills but the actual number of available resources for IT security. This is a challenge that has be tackled by the higher management, since the **return on investment (ROI) in cybersecurity expertise** is definitely high for such critical sectors.

KEY FINDINGS AND RECOMMENDATIONS

The information gathered during Cyber Europe 2018 was analysed by ENISA. This resulted in an extensive list of over **90 concrete observations**. Based on the observations we analysed the consequent **challenges** and **gaps** and proposed **80 detailed recommendations**.

The list below includes the key findings and recommendations from the exercise.

1. EU Member States cooperation at technical level has been improved and proved to be efficient. Minor issues with cooperation structures and tools can be easily treated by the CNW. Regular exercises, trainings and communication checks are important in order to keep the knowledge of procedures and usability of cooperation tools at an adequate level. **Responsible**: CSIRTs Network and ENISA (as the Secretariat).
2. EU-level cooperation at operational-level shall be further developed and tested. Including the interaction between operational and technical levels, and the strategic guidance of higher political management. The procedures and tools needed in order to implement the framework defined in the EU-level coordinated response to large-scale cyber crises (known as the Blueprint) shall be defined and tested. **Responsible**: the actors identified in the Blueprint [1].
3. At national-level countries shall develop procedures and tools for coordinated response, including structured cooperation and information exchange between private actors and public authorities. Special care needs to be taken during the development of such procedures and tools in order to provide incentives to cooperate and exchange information avoiding unidirectional information flow. When such national-level standard operational procedures for public-private cooperation are established, they should be tested by exercises on a regular basis. **Responsible**: National cybersecurity authorities.
4. The private sector shall identify IT security as a priority and invest in resources and expertise. Especially when the services they are providing is essential for the society. **Responsible**: private sector entities of essential or critical services.
5. Organisations, public and private, must ensure that they have crisis communication protocols in place and that employees in sensitive positions are aware of these protocols. **Responsible**: all organisations, private and public, that may be subject to cybersecurity incidents.
6. Cyber Europe has been established as the main EU cyber crisis management exercise. The participants unanimously agreed that the exercise has proven to mature. The challenge is to keep the exercise standards at the highest level. **Responsible**: ENISA and Member State authorities responsible for the planning of the exercise.

[1] Commission Recommendation (EU) 2017/1584, 13 September 2017, on 'coordinated response to large-scale cybersecurity incidents and crises'.

PART I
EXERCISE OVERVIEW

1.1 GOALS AND OBJECTIVES

Cyber Europe 2018 goals built upon those set in Cyber Europe 2016, following an in-depth assessment of their relevance performed in the after action report of the latter exercise [2].

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**.

The goals of the exercise are high level. These have been analysed into concrete objectives that drove the exercise design. The following table presents the decomposition of the exercise goals into objectives.

1.2 TARGET AUDIENCE AND PARTICIPATION

Participation in Cyber Europe 2018 was limited to organisations from the **European Union institutions**, **European Union Member States and European Free Trade Association member countries**, both the **public** and the **private** sectors in these countries.

The main target audience of the exercise was comprised of professionals and organisations involved in information security activities in **the Aviation sector**. Some participants chose to involve players from other sectors as well, as indicated in Figure 3.

In total, **892 participants** [3] officially registered for the exercise, representing the 28 EU Member States, 2 EFTA countries (Norway and Switzerland), several EU institutions and agencies and one international organisation in the Aviation sector (Eurocontrol/ Network Manager [4]).

Out of the total participants, around **60 %** were from the private sector. Figure 3 — Sectorial representation in CE2018 illustrates the percentage of the different sectors representation in CE2018.

[2] https://www.enisa.europa.eu/publications/ce2016-after-action-report

[3] 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 was effectively significantly higher.

[4] https://www.eurocontrol.int/network-manager

Table 1. CE2018 Goals and objectives

Strategic goal	Objective	Metrics/Indicators
G1. Test EU-level cooperation processes	O1. Assess the quality of information sharing	Timeliness, usefulness, structured vs unstructured
	O2. Monitor occurrences of cooperation activities	Number of EU Cyber SOPs cooperation activities held, e.g. meetings/teleconferences, 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 options (to senior management) to follow in a crisis.
G2. Provide opportunities for MS to test their national-level cooperation processes	O5. Provide opportunities to Participants to test their intra-organisational procedures, if they exist (BCPs, Crisis Management Plans, etc.)	Number of opportunities recognised and used by the Participants.
	O6. Provide opportunities to Participants to test cross-organisational cooperation processes, if any	Number of opportunities recognised 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 recognised and used by Participants
G3. Train EU- and national-level capabilities	O8. Provide opportunities to train a wide variety of cybersecurity-related skills	Number of Participants who used the training opportunities, level of satisfaction of Participants in training opportunities
	O9. Provide learning opportunities	Number of learning opportunities recognised by Participants
	O10. Provide self-assessment opportunities	Types of self-assessment opportunities recognised and used by Participants
	O11. Identify training needs for the future	Number of different types of training needs identified

Figure 1. Overall participation in CE2018

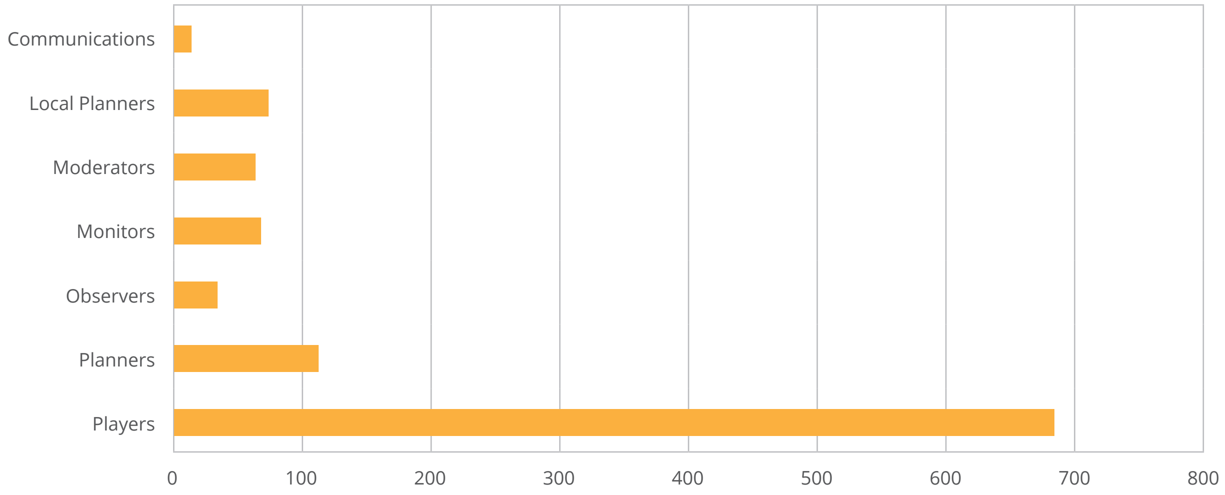


Figure 1. Level of participation per country

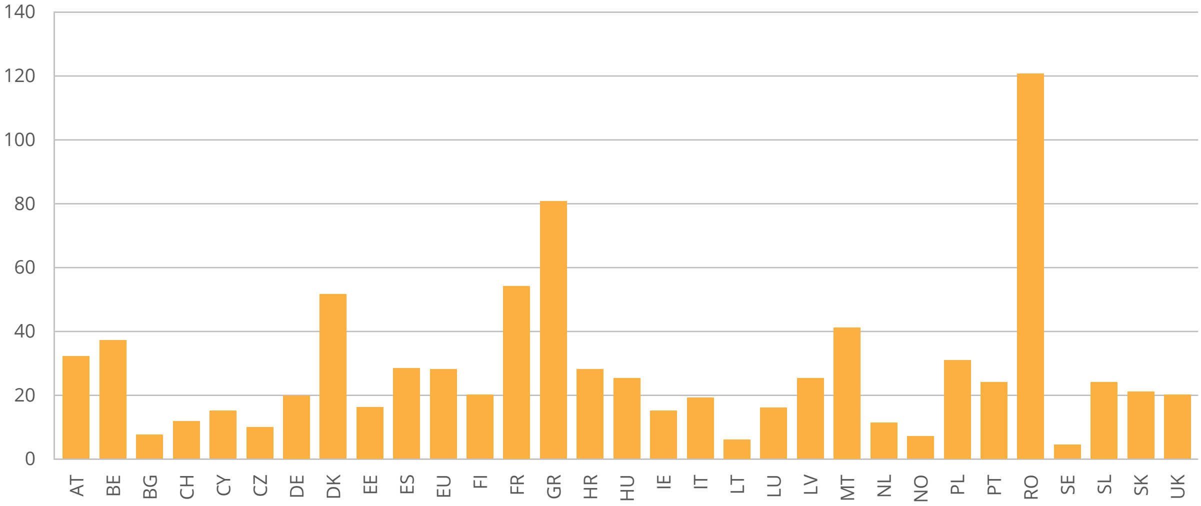
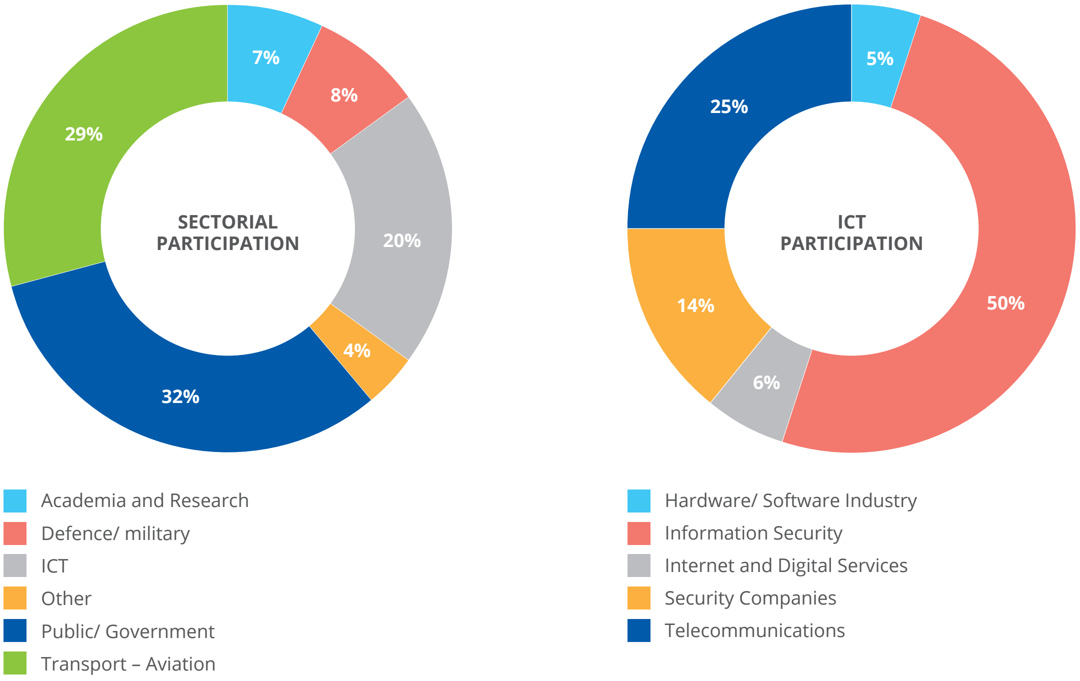


Figure 3. Sectorial representation in CE2018



1.3 PLANNING AND SET-UP

The key planning dates of exercise and delivery were the following:

- 11 May 2017: Initial Planning Conference (IPC);
- 17-18 Oct 2017: Main Planning Conference (MPC);
- Nov-Dec 2017: Invitations to Participants;
- 6-7 Mar 2018: Final Planning Conference (FPC);
- 3 May 2018: Dry-run meeting;
- 6-7 Jun 2018: Exercise Conduct — Distributed/ Exercise Control in Athens;
- 28 Nov 2018: Exercise AAR Conference.

Cyber Europe 2018 followed the same set-up as the second phase of CE2016:

- It was a 2-day distributed exercise, during normal working hours, though the players were allowed to play continuously, as they wished;
- The players were remote, usually at normal place of employment or in incident cells;
- Injects were sent to players based on which they should have reacted appropriately;
- There was a single Central Exercise Control (ExCon) at ENISA in Athens;
- Exercise moderators representing all participating countries supported execution at ExCon;
- Local monitors supported players at national or local level;
- Injects and support was available during normal working hours, though the players were allowed to play continuously, as they wished.

The Cyber Europe 2018 was 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

The scenario was set around the concept of the worldwide rise of extremism. This 'virtually invisible' phenomenon has turned into an open and widespread one with several different facets, from religion to political beliefs, engaging thousands of followers and millions of supporters. The number of radical websites has increased exponentially since 2013 and extremists are utilising social media to recruit and organise.

The increase of the followers of this extremism lead to their engagement in cyber-attacks. Radical groups could use advanced or less advanced techniques to strike at any time as they revealed the internet to be a hotbed of radicalisation; 'Now on the internet, radicalisation can occur instantly and anonymously within significantly larger and more geographically distributed groups'. A new radicalistic movement, without a central organisation has a powerful arsenal of cyber-attack techniques with capabilities, such as exfiltration, traffic capturing and logging, keylogging, ransomware, hybrid attacks with drones, IoT infectors, worms, etc.

The exercise realism was enhanced with a large number of injects being delivered within the Exercise Universe of ENISA's Cyber Exercise Platform (CEP). The Universe included a number of emulated real-world platforms:

- Mainstream media outlets
- Social media
- Websites of key exercise simulated entities
- Yellow pages

The detailed scenario of the exercise consisted of numerous materials 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 multiple simulated platforms**;
- A **simulated news channel**, depicting the event through filmed news in a realistic fashion, supported by simulated **formal news websites** containing **hundreds of news articles and formal news websites**;
- Hundreds of **tailor-made documents** supporting the scenario for Participants to analyse, from technical incident material to legal and public affairs documents.

Finally, during the exercise, live media pressure was simulated by real **journalists** who were continually contacting players to ask for information. **Real-time response** by the experts was noted, while dynamic media reactions in simulated **social media were added** by the journalists.

1.5 EVALUATION

In order to evaluate the exercise against the **objectives and key performance indicators** presented in Section 1.1, ENISA collected feedback from Participants of Cyber Europe 2018, as well as statistics from the different exercise platforms.

- Evaluation survey results (see Annex C);
- Observation and status reports;

- Platforms [5] 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 on the basis of the exercise goals as follows:

- Findings related to EU-level cooperation;
- Findings related to national-level cooperation;
- Findings related to training at national and EU levels;
- Findings related to exercise organisation.

1.6 KEY RECOMMENDATIONS

Based on the findings ENISA proposed 80 recommendations. The key recommendations are given below:

1. EU-level cooperation at technical level has been improved and proved to be efficient. Minor issues with cooperation structures and tools can be easily treated by the CNW. Regular exercises, trainings and communication checks are important in order to keep the knowledge of procedures and usability of cooperation tools at an adequate level. **Responsible**: CSIRTs Network and ENISA (as the Secretariat).

2. EU-level cooperation at operational-level shall be further developed and tested. Including the interaction between operational and technical levels, and the strategic guidance of higher political management. The procedures and tools needed in order to implement the framework defined in the EU-level coordinated response to large-scale cyber crises (known as the Blueprint) shall be defined and tested. **Responsible**: the actors identified in the Blueprint.

3. At national-level countries shall develop procedures and tools for coordinated response, including structured cooperation and information exchange between private actors and public authorities. Special care shall be taken during the development of such procedures and use of tools in order to provide incentives to cooperate and exchange avoiding the negative feelings when information flow seems to be unidirectional. When such national-level standard operational procedures for public-private cooperation are established, they should be tested by exercises on a regular basis. **Responsible**: national cybersecurity authorities.

4. Private sector shall management shall identify IT security as a priority and invest in resources and expertise. Especially when the services they are providing is essential for the society. **Responsible**: private sector entities of essential or critical services.

5. Organisations, public and private, must ensure that they have crisis communication protocols in place and that employees in sensitive positions are aware of these protocols. **Responsible**: all organisations, private and public, that may be subject to cybersecurity incidents.

6. Cyber Europe has been established as the main EU civilian exercise. The participants unanimously agreed that the exercise has proven to mature. The challenge is to keep the exercise standards at the highest level. **Responsible**: ENISA and Member State authorities responsible for the planning of the exercise.

[5] We use the log from the Cyber Exercise Platform as well as the CSIRTs Network cooperation tools, which were used in exercise mode during Cyber Europe 2018.

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 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 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 online www.enisa.europa.eu.

ENISA Athens Office
European Union Agency for Network
and Information Security
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

ENISA Heraklion Office in Crete
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue number: TP-06-18-410-EN-N
ISBN: 978-92-9204-287-5
DOI: 10.2824/369640

enisa.europa.eu