Cyber Europe 2016 – Questions and Answers

Contents

1 What is Cyber Europe 2016?

Cyber Europe 2016 (CE2016) is the largest and most comprehensive EU cyber-security exercise to date. It is a multi-event cyber exercise that involves more than 700 cyber-security professionals from 30 EU and EFTA countries and over 300 organisations, including but not limited to: national and governmental cybersecurity agencies, ministries, EU institutions as well as internet and cloud service providers and cybersecurity software and service providers.

The first phase of the exercise started in April 2016 and will finish in October, focussing mainly on the technical analysis of various cyber security incidents. It was rolled out realistically over a period of 6 months, simulating the build-up of a major cybersecurity crisis in Europe. The second phase, which takes place on the 13th and 14th of October 2016, is the culmination of the first phase, and joins ICT industry experts together with national CSIRTs (Computer Security Incident Response Teams) and the IT security industry to mitigate an unprecedented cyber crisis, to ensure business continuity within the internal single market.

2 What are the objectives of Cyber Europe 2016?

The goals of CE2016 are to test both national and EU-level cooperation in the event of a cyber crisis and to train the capabilities of participants.

Concretely speaking, both phases of CE2016 provide numerous opportunities to improve cybersecurity technical skills, while the second phase also provides opportunities to improve business continuity processes, and test organisational, national and European level cooperation processes.

Ultimately, exercises such as CE2016 enable the European cyber-security community to further build its capacity in identifying and tackling large scale threats, to better understand "cross-border" incident contagion and to reinforce cooperation amongst public and private entities, hereby reinforcing the overall level of cybersecurity in the European Union.

3 Who is participating in this exercise?

Cyber Europe 2016 involves more than 700 cyber-security professionals from 30 EU and EFTA countries and over 300 organisations including: national and governmental Computer Security Incident Response Teams, cybersecurity agencies, EU Institutions, EU agencies, public entities such as ministries of ICT, internet and cloud service providers, cybersecurity software and service providers, banks, energy companies and other critical infrastructure operators. All cyber-security professionals involved in the exercise, public or private, were selected by Member States representatives responsible for the planning of CE2016 at national level.

All 28 European Union Member States participate in the exercise, as well as 2 European Free Trade Association Member States: Norway and Switzerland.

4 How were the participants chosen?

All participants, public and private, were selected by the Member States' national authorities. Employees of European entities who wished to participate had to contact their country's authorities, which then handled their request for participation. According to the exercise policy, employees of entities, public or private, outside Europe, do not participate in this exercise.

5 How is the exercise planned?

Cyber Europe 2016 is organised and coordinated by ENISA and a planning team comprised of representatives from the cybersecurity authorities of the participating counties. ENISA facilitates the planning process by organising various workshops, teleconferences, and training events over the course of approximately 1.5 years.

6 What is the scenario of Cyber Europe 2016?

The Cyber Europe 2016 scenario includes a simulation of a 6-month long crisis with numerous malicious actors involved in multiple realistic yet innovative attacks against European assets. Although the details of the scenario cannot be divulged, it was developed in order to support the exercise objectives to foster national and international cooperation, as well as technical and operational capability development. For this reason, the scenario is based in political and economic policies of relevance to the cybersecurity sector and in particular to the European Digital Single Market[1] and the Network and Information Security (NIS) Directive[2].

Lastly, technical challenges were developed so as to support exercise objectives, but also raise awareness of participants on existing and upcoming attack scenarios. All technical challenges have a basis in recent real-life attacks, or were later technically confirmed by real-life attacks conducted by malicious actors and revealed in the press.

[1] See: https://ec.europa.eu/priorities/digital-single-market_en and https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-role-in-the-european-digital-single-market-dsm

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

7 How were the cyber incidents chosen for the exercise?

ENISA's cybersecurity experts together with experts from the Member States combined real existing cyber-attack scenarios and future trends to create engaging crisis scenarios. Cyber Europe 2016 pictures a very dark scenario, inspired by events such as the blackout in Ukraine in Christmas 2015 or the dependence on technologies manufactured outside the jurisdiction of the European Union. It also features IoTs, drones, cloud computing, innovative exfiltration vectors, mobile malware, ransomware, etc. For the first time, a fully fledged story was developed with actors, media coverage, simulated companies and social media, so as to make the scenario as realistic as possible to those participating.

8 What is general readiness in Europe to deal with cyber-attacks?

The exercise has been designed to illustrate how the cybersecurity sector in Europe has matured over the last few years, in a number of domains technical, operational, political, industrial, economical.

Additionally, the exercise is expected to highlight that strong cross border cooperation is necessary to mitigate large scale cybersecurity incidents. This is still an area for improvement in Europe, as the NIS Directive rightly underlined with the creation of a cooperation network.

International cooperation is essential for Europe. Cybersecurity incidents are rarely confined to the borders of one country, hence it useful/important to test and enhance transnational cooperation at all levels. Transnational cooperation is difficult for numerous reasons: sovereignty, lack of communication channels, lack of capabilities, lack of trust. ENISA plays an essential role in bringing Member States together, and is committed to contributing even further in the coming years.

Activities such as Cyber Europe help to address many shortcomings, and to highlight how critical EU-level cooperation is. We are therefore pleased to have all EU Member States on board, along with 2 EFTA Member States, and over 700 actors overall.

It is our goal that Europe comes out of this exercise each time significantly strengthened.

9 What are the next steps?

The immediate next steps for ENISA and the participants are to analyse what happened during the exercise and what needs to be improved. A public report with the main findings will be made available early in 2017. Detailed lessons learned will be shared with the participants to the exercise in order to establish a list of actions to improve cybersecurity in Europe.

Cyber Europe will follow up in 2018, while a number smaller scale exercises are planned in between.

Last but not least, it is expected that many of the findings of the exercise will influence the implementation of the NIS Directive and the work of the CSIRT Network, the European cyber cooperation platform, but also provide input to the development of a cyber cooperation blueprint as announced[3] by the European Commission

[3] https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

10 What can be done to tackle cyber threats across Europe more effectively?

This is exactly the purpose of such exercises: improve and identify areas where we can become better.

First, undoubtedly there is always the need for increased cooperation. The vast majority of cyber threats can be discussed at European level, which is why the NIS Directive set up processes to further develop this cooperation, and why ENISA supports this activity fully.

Second, we need to reduce the attack surface: this is exactly what the NIS Directive is promoting by establishing minimum security requirements and incident reporting for European critical infrastructure operators. ENISA is playing a key role in this topic for many years and has an important contribution to make in the years to come.

Third, if Member States are already cooperating on a bilateral basis - and sometimes even multilaterally - certain cybersecurity incidents require a pan-European approach. In this sense, no country has authorities with the capacity to liaise with all other countries on a bi-lateral basis. For this reason, we need strong and efficient EU-level cooperation processes and entities, and in particular a strong European cybersecurity agency, ENISA. Lastly, the ongoing discussions on the mandate of ENISA will take into account the lessons learnt from exercises such as Cyber Europe and hopefully pursue the strengthening of EU capacities initiated by the EU cybersecurity strategy and the NIS Directive.

Finally , we need a strong cybersecurity industry. ICT and IT security professionals participated in Cyber Europe 2016 will help to build a strong and robust European industry able to sustain current and emerging threats, ensuring business continuity and creating an environment for businesses to develop within the increasing digitised infrastructures and services.

11 Is Cyber Europe 2016 the first pan-European cyber exercise to take place?

There have already been three pan-European cyber exercises, conducted in 2010, 2012 and 2014.

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. This communication gave birth to the first pan-European Cyber Exercise, which took place on the 4th of November 2010. Cyber Europe 2010 aimed to improve responses to large-scale cyber-attacks through greater communication and collaboration between countries in Europe.

A valuable 'stress test' for European public bodies, CE2010 led to a number of key recommendations, including the importance of private sector involvement in any future exercises, as well as the necessity for Member States to develop national contingency plans that are maintained and tested on a regular basis.

Building on these core lessons, as well as extensive activities at both the national and European level to improve the resilience of critical information infrastructures, Cyber Europe 2012 expanded in scope, scale and complexity. The exercise brought together 29 EU and EFTA Member States as well as several EU Institutions. Overall, 339 organisations participated in the exercise, bringing a total of 571 individual players in action, including private sector actors. CE 2012 produced a series of key findings regarding national-level cooperation, international-level cooperation, and cyber exercises. Crucially, the exercise underscored once more the importance of continuing to develop the European cyber exercise area.

Last, CE 2014 tested for the first time all three levels of incident response: technical, operational and strategic. The largest and most comprehensive EU cybersecurity exercise to that date, CE2014 had three phases that collectively involved over 800 cybersecurity professionals from 29 EU and EFTA countries and 300 organisations. During the first phase of the exercise, conducted on 28th and 29th of April 2014, participants across Europe dealt with 16 different challenging technical cybersecurity incidents. The second phase of the exercise was held on the 30th of October 2014, where 29 EU and EFTA countries cooperated by using the EU-Standard Operational Procedures (EU-SOPs)[4] to establish a common situation picture. The third phase of CE2014, which took place on the 24th and 25th of February 2015, focused on strategic-level cyber crisis management.

12 What were the objectives of the previous exercises?

In a nutshell, all Cyber Europe exercises pursue similar objectives, which revolve around developing cyber capabilities and skills, and fostering cooperation at national and international levels.

In 2010, the exercise fostered mainly operational level capabilities and international cooperation. In 2012, technical capabilities were also tested. In 2014, the private sector participated in a Cyber Europe for the first time, which allowed to also test national cooperation, from the technical to the political level. Cyber Europe 2016 is going a step further, with all these objectives and an additional emphasis on managing the public affairs dimension associated with cyber crises.

13 Will there be a repeat of this exercise in the future?

Cyber Europe is a bi-annual exercise. The next one is planned for 2018.

[4] The objective of the EU-SOPs is to aid in the response to major cyber incidents which can escalate to a cyber-crisis