Cyber Europe 2014 – Questions and Answers

1 What is Cyber Europe 2014?

Cyber Europe 2014 (CE 2014) is the largest and most comprehensive EU cyber-security exercise to date. It is a multi-event cyber exercise that involves more than 400 cyber-security professionals from 29 EU and EFTA countries and 200 organisations, including: Computer Security Incident Response Teams, Cyber Security Agencies, EU bodies, public entities, Telecoms operators, ICT vendors and energy service companies.

Participants of this three phase exercise have to address several technical challenges such as incident detection, investigation, mitigation and information exchanges at technical level. During the first phase of the exercise, conducted in April, participants across Europe dealt with 16 cyber-security incidents. On 30 October, 29 EU and EFTA countries launched the second phase of CE 2014. This operational part of the exercise aims to evaluate updated EU-Standard Operational Procedures (EU-SOPs), the set of contact points, guidelines, workflows, templates, tools, and best practices for managing multinational cyber-crises. The EU-SOPs will be tested extensively and procedures refined according to results. The third and final phase of CE 2014 will take place in early 2015, focusing on strategic objectives.

2 What are the objectives of Cyber Europe 2014?

As a part of Cyber Europe 2014, ENISA, EU Member States and industry will work together to test the resilience of IT systems and response capacity – at a technical, operational and political level – in case of a serious cross-border cyber-security threat.

The scenarios that will be used are based on realistic potential incidents, that aim to test the standard cooperation procedures in the European Union, train and test national-level capabilities, explore the effectiveness of collaboration between private and public players, analyse the escalation and de-escalation processes at all technical, operational, and strategic levels and understand the public affairs issues linked to cyber threats.

More broadly, exercises such as CE 2014 enable the 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 technical cooperation amongst public and private entities.

3 Who is participating in this exercise?

Cyber Europe 2014 involves more than 400 cyber-security professionals from 29 EU and EFTA countries and 200 organisations including: Computer Security Incident Response Teams, Cyber Security Agencies, EU bodies, public entities, Telecoms operators, ICT vendors and energy service companies. These cyber-security professionals were selected by the member states based on the specific nature of the exercise. A strong emphasis was placed on involving the public as well as different parts of the private sector.

4 Which member states/organisation/companies are participating?

ENISA cannot divulge the names of individual bodies or companies, it is up to them to decide.

5 Are all Member States participating?

29 EU and EFTA MS are participating.

6 On what kind of incidents are the CE 2014 scenarios based? What are the main goals of these scenarios ?

The CE 2014 scenarios are based on realistic potential incidents, and were designed to meet the objectives of the exercise, namely:
- To test the Member States and industry working together for resilience of IT systems and response capacity in case of a serious cross-border cyber-security threat.
- To test standard cooperation procedures in the European Union,
- To train and test national-level capabilities, explore the effectiveness of collaboration between private-public and private-private players,
- Finally, its objective is to analyse how the events escalate and de-escalate; to understand these processes at all technical, operational, and strategic levels as well as to understand the related public affairs issues linked to cyber threats.

7 What do you expect this exercise to show in terms of general readiness to deal with cyber-attacks?

It is expected that this exercise will demonstrate that strong cross border cooperation is necessary for the Member States, and the public and private sector. We are therefore pleased to have 29 EU and EFTA member states participating, and over 600 actors involved. This kind of cooperation between EU and EFTA countries is essential for the strengthening of transnational cyber-incident management. The importance of this exercise is to build trust between actors in Europe, to exchange best practice in procedures, cyber exercises, lessons learned, expertise which are all crucial to ensuring a stronger community that is able to tackle transnational cyber-crises. Moreover, the European cyber-incident management community has been further strengthened with input from other critical sectors that are relevant for the management of large-scale crises. So, in short, we will come out of this exercise significantly strengthened.

8 When will the results of the exercise be announced?

Cyber Europe 2014 is a three phase exercise. The aggregated results will only be announced in overarching terms at the end of the year, and as you may understand we cannot divulge any greater details, as to not to hamper the remaining phases of the exercise, or to release any matter which is sensitive and needs to be addressed.

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

It is ENISA’s aim that further exercises will take place in the future. It is the intention that Cyber Europe exercises are conducted every two years. Cyber crisis cooperation and response in Europe are maturing. These exercises are very effective tests of our systems and preparedness, and provide invaluable feedback for making improvements.

10 How is the exercise planned?

Cyber Europe 2014 is organised and coordinated by ENISA and an EU planning team which consists of representatives from the participating countries. ENISA facilitated various workshops, teleconferences, and training events to support the process. Planning team members also formed a number of special “taskforces”. Each taskforce was responsible for a specific part of the planning and preparation of the exercise.

The technical part of the exercise takes places in a distributed manner across all of Europe.

11 How was this influenced by the cyber-attacks of e.g. Russia/Ukraine?

It was not influenced, even if we can understand that some may think so. This has been planned for a long time, and is a biannual exercise.

12 What are the next steps?

Work will continue in this area. Large-scale cyber incidents are rare, so exercises are essential as a way of being able to be ready if a real crisis occurs. Experience from exercises forms the basis for further preparation – particularly in the development of operational plans and making sure sufficient people and resources are available. The exercises take place as part of a “lifecycle” – plans developed from lessons learnt in exercises are themselves tested in future exercises. The aim is to ensure that, in the event of an actual crisis, the operational “routines” that ensure the optimal effective response are in place.

13 What’s the relevance of pan-European cyber exercises in the current socio-economic context?

ICT is the backbone of every modern society. For the sake of Europe’s economy, ensuring its security must therefore be on the political agenda for governments and industry.

Cyber crises are occurring on larger scales and growing more transnational in origin and effect. Moreover, the nature of cyber-threats is rapidly changing. The emergence of big data and new online services is creating increased vulnerabilities. Large-scale information losses and breaches of user data have emerged as a top threat and concern for citizens.

Cyber-attacks are becoming more sophisticated. Simple experiments are now turning into sophisticated activities performed for profit or political reasons. The large number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem.

Society is highly dependent on ICT systems, on Critical Information Infrastructures, such as power plants and transportation systems. Their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face is crucial for the economy of Europe, and raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks.

Managing this evolving threat landscape effectively requires international cooperation. The world is ever more connected (by online networks and services) and therefore international cyber co-operationi s required to support and protect the information society we live in and the economy we live in.

Cyber exercises are an important tool to improve and focus on large scale cyber crisis cooperation. Such exercises enable the 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 technical cooperation amongst public and private entities.

14 Is cyber security preparedness important for the European Union?

Supporting EU-wide cyber security preparedness exercises is one of the main actions of the European Commission’s Digital Agenda for Europe and the latest policy document on European Cyber Security Strategy and proposed directive. Strengthening Europe’s cyber defence and combating potential online threats to essential infrastructure helps ensure that businesses and citizens feel safe and secure online. Moreover, making the best possible use of ICT could help speed up economic recovery and lay the necessary foundations for a sustainable digital future.

15 In your opinion, what is the state of play in Europe today with regard to cybersecurity?

Let us first understand the context: ICT is the backbone every modern society. . For the sake of Europe’s economy, ensuring its security must therefore be on the political agenda for governments and industry. Europe is increasingly addressing these cyber security challenges at a higher political level of awareness, with the EU's NIS directive, its Cyber Security strategy and the strengthening of ENISA. Given the increasing number of cyber-attacks which are becoming more sophisticated, with more resources, time and people being used, this is also logic. The large number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem.

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

There is a need for more European cooperation. That is also the purpose of such exercises, to constantly improve and identify areas where we can become better. One such area is in the communication between different actors; this can always be developed. Europe is such a vast and differentiated landscape, so it is a challenge to grasp how all actors work and to understand their modus operandi. The cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face is crucial for Europe’s economy. It also raises the need to address their security and resilience in a systemic perspective as the first line of "defence" against failures and attacks.

17 Is Cyber Europe 2014 the first pan-European cyber exercise to take place?

No, there have already been two pan-European cyber exercises, conducted in November 2010 and 2012 respectively.

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 rise to the first pan-European Cyber Exercise, which took place on 4 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, CE 2010 produced 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.

18 What were the objectives of the previous two exercises?

The European Commission's 2009 communication on Critical Information Infrastructure Protection (CIIP) gave rise to the first pan-European Cyber Exercise. Cyber Europe 2010 aimed to improve responses to large-scale cyber-attacks through greater communication and collaboration between countries in Europe and involved mainly the public sector.

Building on the core lessons of this exercise, 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 private as well public sector collaborated during the exercise at national and European level.

CE 2012 had three objectives:
- Test the effectiveness and scalability of mechanisms, procedures and information flow for the cooperation of public authorities in Europe.
- Explore the cooperation between public and private stakeholders in Europe.
- Identify the gaps and challenges in the more effective handling of large-scale cyber-incidents in Europe.

19 What were the main recommendations and lessons-learned from these previous exercises?

A valuable 'stress test' for European public bodies, Cyber Europe 2010 produced 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. 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.

CE 2012 demonstrated that continued cooperation between EU and EFTA countries is essential to strengthening transnational cyber-incident management. The exchange of best practices in cyber exercises, lessons learned, expertise and the organisation of conferences are all crucial to ensuring a stronger community that is able to tackle transnational cyber-crises. Moreover, the European cyber-

incident management community could be further strengthened with input from other critical sectors –health, transportation – that are relevant to the handling of large-scale crises.
CE 2012 also illustrated the value of the ongoing involvement of the private sector in this and the future exercises and the importance of exploring inter-sectorial dependencies and focusing more on specific communities.

20. On what real-life incidents are the scenarios based? Why were those incidents chosen for the exercise? How will this exercise actually work?

These scenarios are based on realistic potential incidents, and were designed to meet the objectives of the exercise, namely:
- to test the Member States and industry working together for resilience of IT systems and response capacity in case of a serious cross-border cyber-security threat.
- to test standard cooperation procedures in the European Union,
- to train and test national-level capabilities, explore the effectiveness of collaboration between private-public and private-private players,
- Finally, its objective is to analyse how the events escalate and de-escalate; to understand these processes at all technical, operational, and strategic levels as well as to understand the related public affairs issues linked to cyber threats.

21. When will the results CE2014 OLEx be announced?

Aggregated results from the three phases of CE2014 will only be announced in overarching terms after the end of the third phase (strategic) and as you may understand we cannot divulge any greater details, as to not to hamper the following phases of the exercise, or to release any matter which is sensitive and needs to be addressed.

22. How were the organizations/companies participating chosen, or did they volunteer to take part? Did any organizations or governments chose not to take part and, if so, why?

The participants were selected by the MS based on the nature of the exercise. ENISA wanted to have a strong involvement of the public and different parts of the private sector.
On the latter, this is not information we have access to, as it was in the hands of the MS.

23. What do you expect this exercise to show in terms of general readiness to deal with cyber-attacks?

It is expected that this exercise will demonstrate that a strong cross border cooperation is necessary for the Member States, and the public and private sector. We are therefore pleased to have 29 EU and EFTA member states participating, and over 600 actors involved.
This kind of cooperation between the EU and EFTA countries is essential for the strengthening of transnational cyber-incident management. The importance of this exercise is to build trust between the actors in Europe, to exchange best practice in procedures, cyber exercises, lessons learned, expertise which are all crucial to ensuring a stronger community that is able to tackle transnational cyber-crises.
Moreover, the European cyber-incident management community has been further strengthened with input from other critical sectors that are relevant for the management of large-scale crises.
So, in short, we will come strengthened out of this exercise.

24. In your opinion, what is the state of play in Europe today with regard to Cyber-security? Where do you see gaps in coverage? In which area things could be handled better?

Let us first understand the context: ICT is the backbone every modern society, thus security must be on the political agenda for governments and industry, for the economy of Europe. Europe is increasingly addressing these cyber security challenges at a higher political level of awareness, with the EU's NIS directive, its Cyber Security strategy and the strengthening of ENISA.

Given the increasing number of cyber-attacks which are becoming more sophisticated, with more resources, time and people being used, this is also logic. The large number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem.

There is a need for more European cooperation. That is also the purpose of such exercises, to constantly improve and identify areas where we can become better. One such area is in the communication between different actors; this can always be developed. Europe is such a vast and differentiated landscape, so it is a challenge to grasp how all actors work and to understand their modus operandi.

The cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face is crucial for the economy of Europe. It also raises the need to address their security and resilience in a systemic perspective as the first line of "defence" against failures and attacks.