Cyber Europe 2010 – Evaluation Report

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of expertise for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Acknowledgments

While compiling this report, we gathered input from the exercise players and the Member State moderators. ENISA would like to express its gratitude to the stakeholders that provided input to the report.

Many thanks also to the 4C Strategies team that helped to gather the material and supported drafting this report.

Contact details

For more information about this report, please contact:
Dr. Panagiotis Trimintzios
Network Resilience and CIIP
ENISA
resilience@enisa.europa.eu
http://www.enisa.europa.eu/act/res

Legal notice

Table of contents

Executive summary

Executive summary

The first pan-European exercise on Critical Information Infrastructure Protection (CIIP) CYBER EUROPE 2010 was organised by EU Member States (MS), facilitated by the European Network and Information Security Agency (ENISA) and supported by the Joint Research Centre (JRC).

The objective of the exercise was to trigger *communication* and *collaboration* between countries in Europe to try to respond to large-scale attacks. During the CYBER EUROPE 2010 exercise, experts from the participating public bodies of European countries worked together to counter simulated attempts by hackers to paralyse the Internet and critical online services across Europe.

The simulation exercise was based on a *fictitious* scenario on a *fictitious* Internet interconnection infrastructure, with a limited number of Internet Interconnection Sites (IIS[1]) between countries. During the exercise, Internet connectivity between European countries was gradually lost or significantly reduced, requiring cooperation between Member States to avoid a total network crash.

The exercise was a first, key step for strengthening Europe's cyber defences and vital for the common goal to combat potential online threats to essential infrastructure, so ensuring that businesses and citizens feel safe and secure online. Supporting EU-wide cyber security preparedness exercises is one of the priorities of EU policies, in particular of the Digital Agenda for Europe.

The interim findings and recommendations of participating EU Member States in this first pan-European cyber security exercise indicate that CYBER EUROPE 2010 was a useful 'cyber stress test' for public bodies in Europe. Member States are keen to continue their efforts in the area of national and pan-European exercises. They also agree on the importance of involving the private sector in future exercises and exchanging lessons learnt with other national or international exercises.

The exercise was conducted from 10:00am - 17:00pm CET on the 4th of November and was followed by an Exercise Debrief session on the following day. The exercise was organised as a distributed table-top exercise, with players participating from their office locations and as part of their daily routine. Participants from 30 countries (EU and EFTA) were represented in CYBER EUROPE 2010; 22 countries were actively playing, while eight countries were present as observers, having access to exercise happenings and findings. There was a central exercise control organisation in place, Exercise Control (EXCON), situated in Athens, which provided direction and guidance for the exercise. EXCON included the MS-moderators, one representative from each participating country, and the EXCON-moderators, ENISA and JRC, which had overall control of the exercise.

This is the evaluation report that ENISA prepared for the exercise. It is based on analysis undertaken from: i) the EXCON-moderators' observations; ii) the outcomes of individual assessment reports completed by Member States (moderators and players); and iii) the Exercise Debrief discussions on the 5th of November. This report does not represent a consensus from all participating stakeholders. Each MS had their separate internal report, evaluating the experience each received. This report represents ENISA's view of the happenings, based on information gathered during and after the exercise. As such, the view is limited to being based on available information and, of course, on the subjective views of the EXCON-moderators.

The main recommendations include the following:

- The private sector will provide value in future exercises by increasing the realism (c.f., fictitious infrastructure, scenario)
- Exchange lessons-identified with other (national or international) exercises

1 Internet Interconnection Site is a term used only for the purposes of the exercise and does not represent a term used in reality. In reality, such sites are either at Internet Exchange Points or at private peering sites.

- Member States should be well organised internally, for example by developing national contingency plans, which are maintained and tested on a regular basis through national exercises

- A roadmap for pan-European exercises and preparedness should be created. This will include the definition of standard procedures and structures that should be used in the case of large scale events, such as CYBER EUROPE 2010.

The more detailed lessons learnt from the exercise can be summarised in the following three areas:

The planning and structure of the exercise

- The planning phase of the CYBER EUROPE 2010 exercise benefited from the interaction among the participants, which allowed the interests and concerns of all parties to be taken into account and enabled a fruitful and highly appreciated exercise. The hard work of the planners group was essential for this success

- The planning of CYBER EUROPE 2010 should involve increased resources, which will help organisers to involve more external professional support

- The careful preparation of the implementation detail, e.g. technical exercise set-up, the participants' training and the exercise Dry Run were instrumental in the effective and smooth exercise execution

- The exercise set-up and scenario were balanced and were received well by the participants, since they enabled a varied level of activity during the exercise. The level of activity peaked during the first part of the day and slowed down during the afternoon

- It was a key success factor that MS-moderators were located at the same premises and were gathered in the same room

- The high level of activity, the contacts that were established and the overall communication between participants testify to the fact that the overall goal of the exercise was reached

Trust building

- Member States should continue to work on the points of contact that were established during the exercise and to establish a solid European CIIP-network. The consolidation of trust between MS and partners should be a continuing objective

- Member States should continue to organise pan-European exercises in the area of CIIP, because they have proved to be an effective trust building measure

- Future exercises could use 'pre-exercise conference' for players as a mean of creating common knowledge and understanding on different exercise elements. Improvements could also be made by considering/mapping how each Member State is connected to other Member States. Such conferences could be organised at national level by the Member States

- ENISA should help facilitate the establishment of an information exchange mechanism to promote a culture where information can be easily and quickly shared

- ENISA should help facilitate the creation of smaller sub-groups within the area of CIIP. Smaller and more focused groups will ease the discussion of specific topics and the identification of solutions to different problems

- Member States should organise debriefing meetings with their players to further facilitate trust building. This could be done back-to-back with other meetings (for example a CERT-meeting), when people were already present

Increase understanding

- The exercise increased in several ways the understanding of how cyber incidents are handled, both on a European level (between Member States) and on a national level (between players). It is, however, worth mentioning that the artificiality of the scenario limited this scope of understanding to a certain extent. A more realistic scenario could lead to a deeper insight of how cyber incidents are handled
- On a national level, the degree of understanding depended on the level of agency involvement and the number of people participating from each Member State. It was, nonetheless, clear that the actual communication between players helped to increase understanding of the issues at hand. A deeper understanding could have been reached if national pre-exercise workshops had been conducted during the planning phase
- Exercises could be complemented by conferences and seminars. It is, however, important not to duplicate existing structures and programmes
- Member States should increase their knowledge regarding how each Member State handles its crisis procedures. Aligning the procedures could be a step towards effective pan-European crisis management
- Information exchange between Member States on how they handle cyber incidents and crisis situations nationally is of paramount importance. Such information exchange could be done through dedicated workshops
- National contingency plans should be developed and tested on a regular basis through national exercises
- The exercise has shown that the procedures on how to handle cyber incidents do not yet exist on a pan-European level. Such procedures need to be identified and tested in future such exercises

The ability to find points of contact

- The exercise accentuated the necessity to be able to establish and locate relevant points of contact within Europe. Since each country is organised differently, it is very important to know who to contact in case of an incident or, more generally, who is able to answer a specific question
- The ability to find the relevant points of contact varied between and within Member States. In the event of a real crisis, some 55 % of Member States were not confident that they would be able to quickly find the relevant CIIP organisation/s in the appropriate Member State, even with the available directories
- Member States considered that the most important characteristics of a truly useful directory were to be easily available, up-to-date, clear, well-structured and to contain detailed information
- ENISA should keep the latest versions of the directories that were used in the first part of the exercise (CIIP Meridian, ENISA Who-is-Who) available to Member States through the exercise portal
- European countries are organised nationally in a variety of ways. Given the differences in structures and process, it is very important to know who to contact in case of an incident or, more generally, who is able to answer a specific question
- The dialogue on the necessity of Single Point of Contact or Multiple Points of Contact at the EU level should continue. ENISA can be the facilitator of this dialogue.

Efficient communication and data exchange

- The exercise demonstrated the need for efficient communications, leading not only to greater understanding, but also illustrating the differences in structure between Member States. How to achieve efficient communication will need more gathering of requirements and analysis work
- Trust building measures should continue to be developed, as they are closely connected to efficient communication at both national and European level

- It is important that Member States and agencies are able to meet face to face in different forums (for example during exercises, seminars and conferences). The better the relevant actors get to know their counterparts, the more efficient the communication will be

- The exercise highlighted that Member States communicate in a wide variety of ways. Harmonisation would lead to a more secure and efficient communication between Member States. Some form of secure communication would be advisable, for example PGP

Recommendations for future exercises

The dialogue with the Member States will be extended to: include topics for future exercises; create future scenarios based on their input; create a roadmap for more complex exercises.

- It is recommended that Member States draw up a strategic roadmap for future exercises in conjunction with the general strategic planning of their operations. Such an exercise programme should be developed in accordance with Member States' priorities and facilitated by ENISA

- More exercises should be organised on national and bilateral bases. In this respect, the ENISA Good Practice Guide on National Exercises could be utilised

- It is not currently clear if the next exercise should be table top or have more operational character. The second pan-European exercise on CIIP could be an exercise that enables the testing of procedures and ensures preparedness of people to follow them. As the target is to foster communication and collaboration between countries, a purely operations based exercise may diminish the importance of cooperation, leading to a competitive environment

- Future exercises could use 'pre-exercise conferences' for players, organised by Member States as a means of creating common knowledge and understanding of different exercise elements. Improvements could also be made by considering/mapping how each Member State is connected to others. Furthermore, the planning process for future exercises should include the Dry Run concept

- Future exercises would also benefit from a longer planning phase, with fixed deadlines and deliverables. All participating Member States should be members of the planning team

- Future exercises might, moreover, benefit from the inclusion of a private sector component, although the nature of its involvement requires additional consideration. Exchanging lessons-identified with other (national or international) exercises would also be useful

- The exercise has shown that the procedures on how to handle cyber incidents do not yet exist on a pan-European level. Such procedures need to be identified and tested in future such exercises

BER EUROPE
2010
BER EUROPE

Introduction

Introduction

Background

Reliable communication networks and services are critical to public welfare and economic stability. Intentional attacks on the Internet, network disruptions caused by physical phenomena, software and hardware failures and human mistakes all affect the functioning of public communications networks.

The first pan-European exercise on CIIP, CYBER EUROPE 2010, was conducted on the 4th of November 2010. The exercise was organised by EU Member States with support from the European Network and Information Security Agency (ENISA) and the Joint Research Centre (JRC).

This evaluation report is based on analysis undertaken from: i) the EXCON-moderators' observations; ii) the outcomes of individual assessment reports completed by Member States; and iii) the Exercise Debrief discussions on the 5th of November.

Policy context

The European Commission Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM (2009)149 of 30 March 2009, Action Plan states that: "The Commission invites Member States to organise regular exercises for large scale networks security incident response and disaster recovery..."

The Tallinn Ministerial Conference, which took place in April 2009, built on the five pillars of the CIIP Action Plan and stressed that: "A joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan..."[2]

As a final ratification of the importance of exercising, at national but also at a pan-European level, the Council Resolution published in Dec 2009 mentions that: "Member States should organise national exercises and/or participate in regular European exercises in the area of Network and Information Security...", "...ENISA participate with Member States on exercises to provide appropriate responses to emergencies..."

Supporting EU-wide cyber security preparedness exercises is one of the main actions of the Digital Agenda for Europe, the new policy plan of the European Commission.

ENISA's new proposed mandate also highlights the importance of cyber security preparedness exercises in enhancing trust and confidence in online services across Europe.

About the exercise

The exercise was conducted between 10:00am - 17:00pm CET on the 4th of November 2010, followed by an Exercise Debrief the next day.

Delivered as an educational and preparedness activity, the exercise was organised as a distributed discussion based (table top) exercise, with players participating from their own offices, as part of their daily routine. The exercise was coordinated by an MS-moderator for each participating Member State. There was also a central exercise control organisation in place, EXCON, focused on supporting the flow of the exercise (see Figure 1 – Exercise organisation - overleaf).

2 http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf

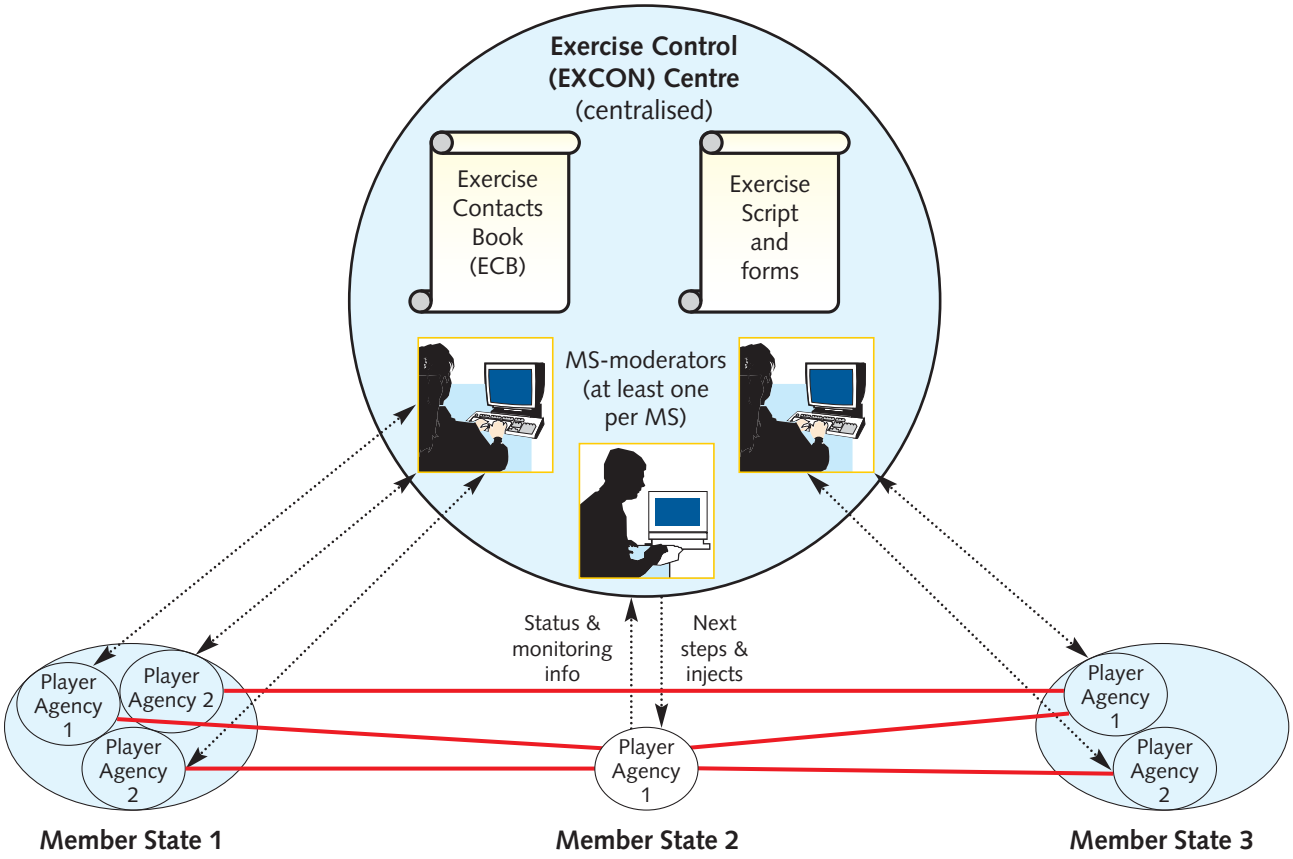


Figure 1: Exercise organisation

Participation

Participating were 22 Member States as players and eight Member States as observers (EU and EFTA). In all, approximately 50 people were present in the Exercise Control Centre, situated in Athens, being exposed to more than 320 so called 'injects' related to the availability of Internet and corresponding critical online services. Across Europe in the participating Member States, around 80 people were acting upon the instructions of their national MS-moderators in Athens. Typical profiles of players were Computer Emergency Response Teams (CERT), Ministries, National Regulatory Authorities, Intelligence Services, Cyber-Crime Units, etc.

Main objectives and measures tested

The aim of CYBER EUROPE 2010 was to explore, through a table top exercise, the response to incidents that compromised the resilience of the Internet. The incidents affected all participating Member States.
The main objectives of the exercise were:

- To build trust
- To increase the understanding among Member States of how cyber incidents are handled.

Within the overarching objectives, CYBER EUROPE 2010 was intended to evaluate:

- The ability to find relevant points of contact in the EU
- The communication efficacy and the type of data exchanged (on a national and European level).

The exercise partly helped to answer the following questions:

- What further trust building measures can be taken on a national and European level within the area of CIIP?
- How can we further increase the understanding among Member States of how cyber incidents are handled?
- How can we further enhance the ability to find points of contact within Europe?
- How can we increase the efficiency of communication within the area of CIIP?

Exercise planning

Exercise planning

The planning, delivery and evaluation of the exercise was coordinated by ENISA with the support of the JRC. The process ran from the beginning of January 2010 through to the exercise date.

The workshops

The overall process for the planning and delivery of CYBER EUROPE 2010 was managed via a series of workshops, held together with the Member States:

- 1st Workshop, 28th January 2010, Brussels
  - In this workshop, the participants agreed on the exercise objectives and set the main principles
- 2nd Workshop, 11th March 2010, Brussels
  - In this workshop, the participants agreed on the detailed planning of the exercise and identified the high-level scenario around which the exercise scenario would be built. It was during this workshop that the team of planners from Member States was established. Its members would work together very closely in order to plan the overall exercise
- 3rd Workshop, 12th May 2010, Tallinn
  - In this workshop, the participants were presented with the work of the planners regarding the exercise set-up, the detailed scenario, and the policies about media and observers. The participants agreed with the proposals in general and gave feedback to the planning team to continue their efforts
- 4th Workshop, 28th Jun 2010, Brussels
  - In this workshop the participants presented their national organisation and procedures related to CIIP crisis. The workshop triggered discussions between the participants and took further steps towards understanding each other and increasing trust
- 5th Workshop, 24th Sep 2010, Athens
  - The 5th workshop was dedicated to the training and preparation of all the exercise moderators (MS-moderators and overall EXCON-moderators). It took the form of exercise training, leading to a Dry Run. Representatives from 21 countries participated, while observers were not invited in this first phase. The objectives of the exercise training and Dry Run were to: increase understanding of the exercise set-up and methodology, verify functionality and quality of the communication platform, and to increase familiarity and knowledge within the moderators' group

Exercise documentation

The following documents were provided before the exercise:

- Information package for MS-moderators and for players:

The aim of the information package was to present common directives and guidelines for the preparation, execution and evaluation of the exercise. In the documents, the MS-moderators and national players had access to information regarding the purpose and goal of the exercise, exercise guidelines and directions on exercise roles and responsibilities. Additionally, exercise documentation included:

- A set of slides for the MS-moderators, to be used to brief national players on the set-up of CYBER EUROPE 2010
- A list of frequently asked questions for national players

- Evaluation forms for MS-moderators and for national players
- Status form

The status form was filled in by MS-moderators on an hourly basis during the exercise and was forwarded to the EXCON-moderators. The MS-moderators gathered the required information from players either by using the same form or by any other means they preferred.

Planners group

A planners group was created to help plan the exercise and give guidance about relevant issues. The planners group was composed of experts from eight Member States (DK, FI, FR, HU, IT, PT, SE, UK), ENISA and JRC. The planners group was instrumental in the creation of the scenario, observer and media policy. It also provided valuable feedback and input on the draft versions of the exercise documentation (for example, the information package for MS-moderators and for players, as well as the evaluation and status forms).

ENISA facilitated the overall process, managing the preparation, execution and evaluation of the exercise, as well as making recommendations based on lessons identified.

JRC provided scientific and technical support, including the communication and coordination tool that made the exchange of hundreds of simulated events possible. The scale and the distributed nature of the exercise imposed extensive requirements in terms of coordination and communication efficiency.

Policy documents

A number of policy documents were established to give guidance on certain specific issues. The documents were:

- Media policy

The media policy gave direction regarding media presence during the exercise and on the content and timing of press releases before and after the exercise.

- Observer policy

The observer policy outlined basic principles for the observers, described the approval process, as well as the observers' rights and obligations. The policy also highlighted what role the observers were going to be given during the exercise and during the exercise evaluation.

- 'No Play' policy

The 'No Play' policy was created to handle the event of withdrawal of a MS or playing agency from the exercise.

A portal was set-up by ENISA to store the exercise documentation in a secure environment, and mailing lists facilitated the preparation work of the moderators and planners. The policy documents should be reviewed for future exercises, possibly enabling observers and other external stakeholders to be more active.

BER EUROPE
2010
BER EUROPE

Scenario and the execution of the exercise

Scenario and the execution of the exercise

The exercise was structured around a scenario that included several incidents compromising the resilience of the Internet. The incidents affected all participating countries. The scenario of CYBER EUROPE 2010 was developed to trigger communication between MS. The overarching idea driving this scenario was an attack on critical assets that would impact all participating MS.

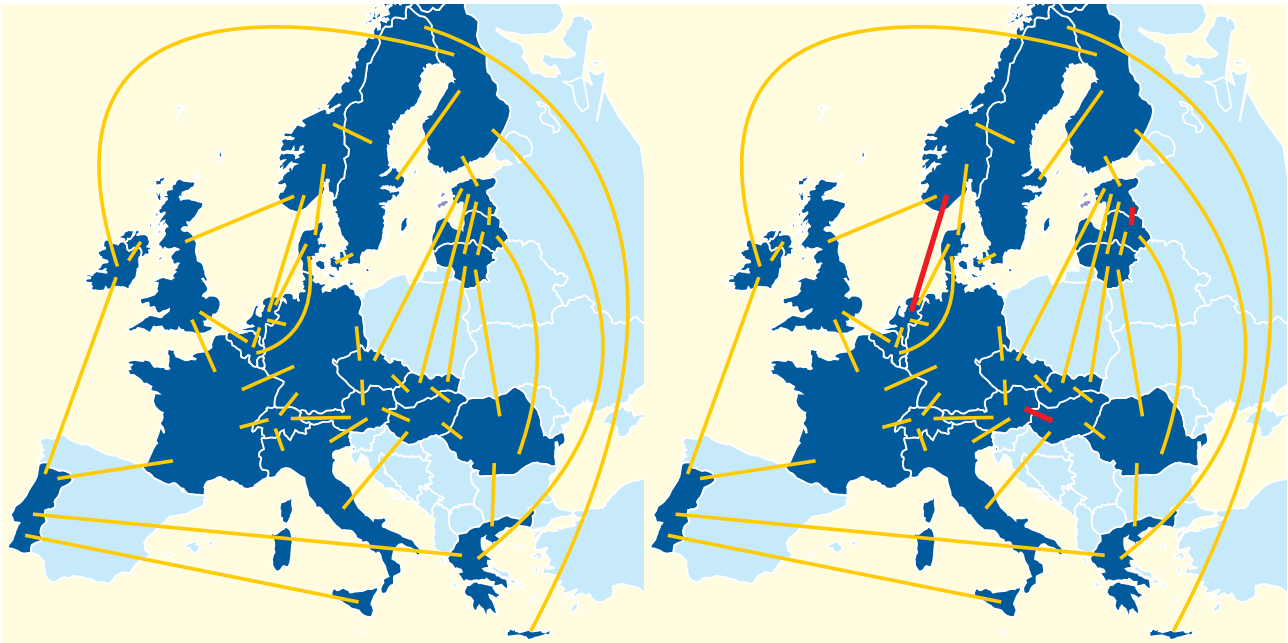
The main phases of the exercise were the following:

1) **Discovery phase:** i.e. to find points of contact in available directories, understand the exercise set-up, etc.
2) **Attack phase:** i.e. several attacks against cross border Internet Interconnection Sites (IIS) to trigger the need for communication between Member States.
3) **Recovery phase:** i.e. problem resolution triggers the need for communication between Member States, in order to resume normal activity.
4) **Wrap up phase:** i.e. Member States are asked to issue a short report on cooperation activities.

The overall scenario concentrated on the contingency phase after the attack since, in reality, the main actors involved during the initial stages of the attack would primarily be from the private sector. The exercise did not attempt to simulate the actions of the private sector, nor did it attempt to engage participants in acting as the private sector. Accordingly, the scenario started at the point at which public bodies were involved, focusing on the public sector component of incident response.

The general theme of the scenario

In CYBER EUROPE 2010, experts worked together to counter simulated attempts by hackers to paralyse Internet Interconnection Sites (IIS) and critical online services in several European countries. The topology of the IIS network was deliberately fictitious. The simulation was based on a scenario where Internet connectivity between European countries would be gradually lost or significantly reduced in all participating countries, so that citizens, businesses and public institutions would find it difficult to access essential online services. In the exercise, Member States needed to cooperate with each other to avoid a simulated total network crash. The loss of Internet connectivity during the exercise is visualised by the maps below.



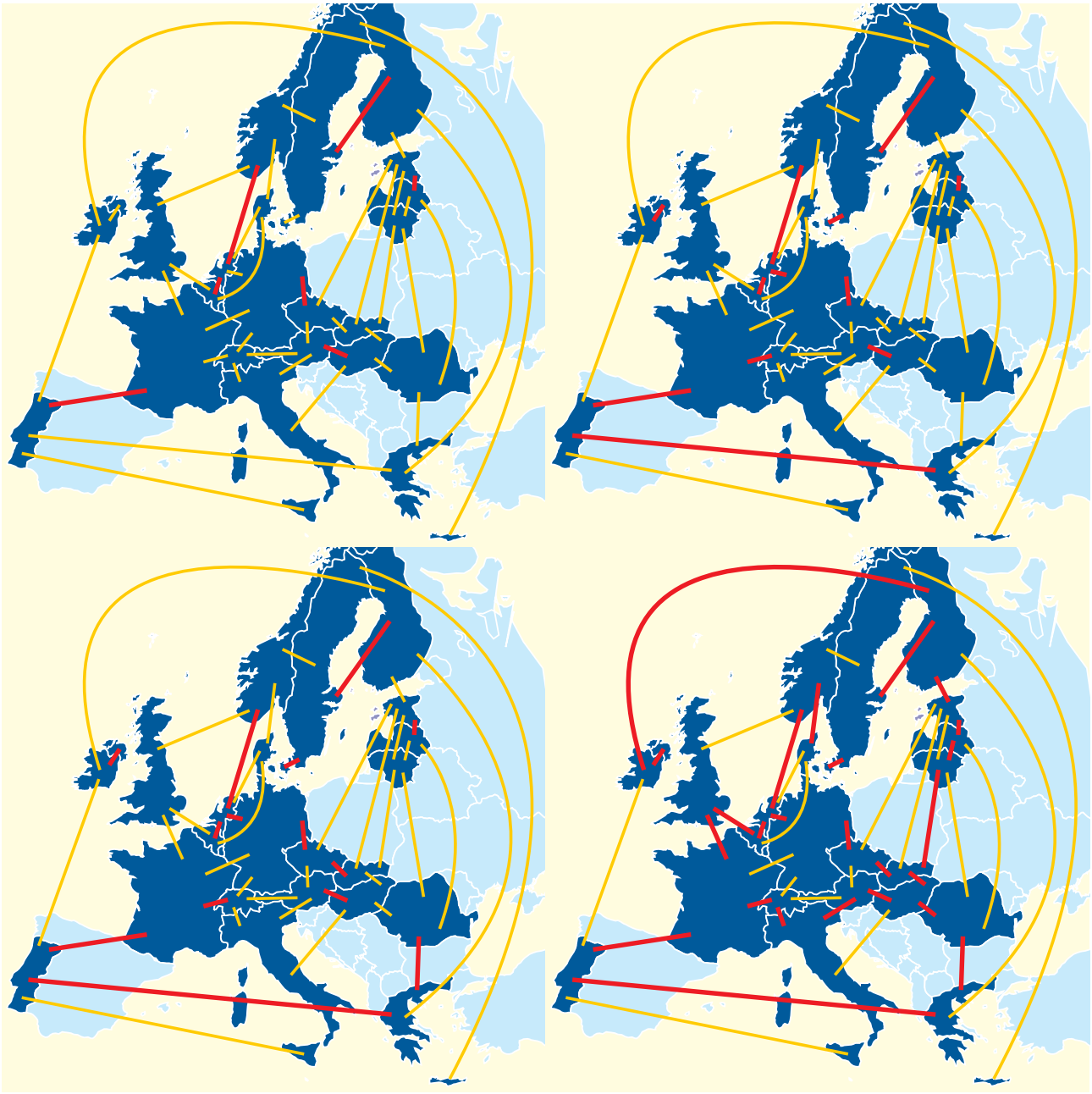


Figure 2: Maps showing the gradual loss of Internet connectivity

Main Scenario Event List (MSEL)

The Main Scenario Event List (MSEL) contained the substance of the scenario and was administered by the EXCON-moderators in order to manage the exercise.

- All injects had predefined 'senders', for instance:
  - CERT
  - Intelligence
  - Media
  - Web site admins
  - EXCON (exercise related)

- All injects had predefined recipients and, accordingly, were not sent to all 'recipients', nor were they sent simultaneously. For example, injects were sent to:
  - All players
  - All players in a MS
  - Only law enforcement agencies

- The exercise coordination and communication platform was structured around a portal that automatically provided to the MS-moderators the injected events in a timely fashion and according to the MSEL

Additional scenario information

- Players were able to request additional information regarding different aspects of the scenario

- In order to provide a good exercise for the players, EXCON had a number of prepared documents that could be either:
  - Sent to players
  - Used by MS-moderators as background information when talking to players

- Background documents could be found on the portal
  - The documents included more information on hackers, operators, media, attack initiation, etc.

- EXCON-moderators provided direction and guidance about the timing and the mechanism of distribution of documents to the players

Exercise Dry Run

As mentioned previously, an exercise Dry Run was held on September 24th, 2010. During this event, the usability of the communication platform was tested, as well as the interaction between EXCON-moderators, MS-moderators and players. Furthermore, MS-moderators were introduced to a scenario similar to that which was to be used during the actual exercise.

The Dry Run was perceived by MS as an important and effective mechanism for training and for resolving any issues related to exercise technicalities and tools. Figure 3 below shows that 87% of the MS-moderators thought that the Dry Run was extremely or very useful as a precursor to the exercise.

The Dry Run concept should be included in the planning process of future exercises. It should also be considered whether a Dry Run scenario should be more similar to the exercise scenario.

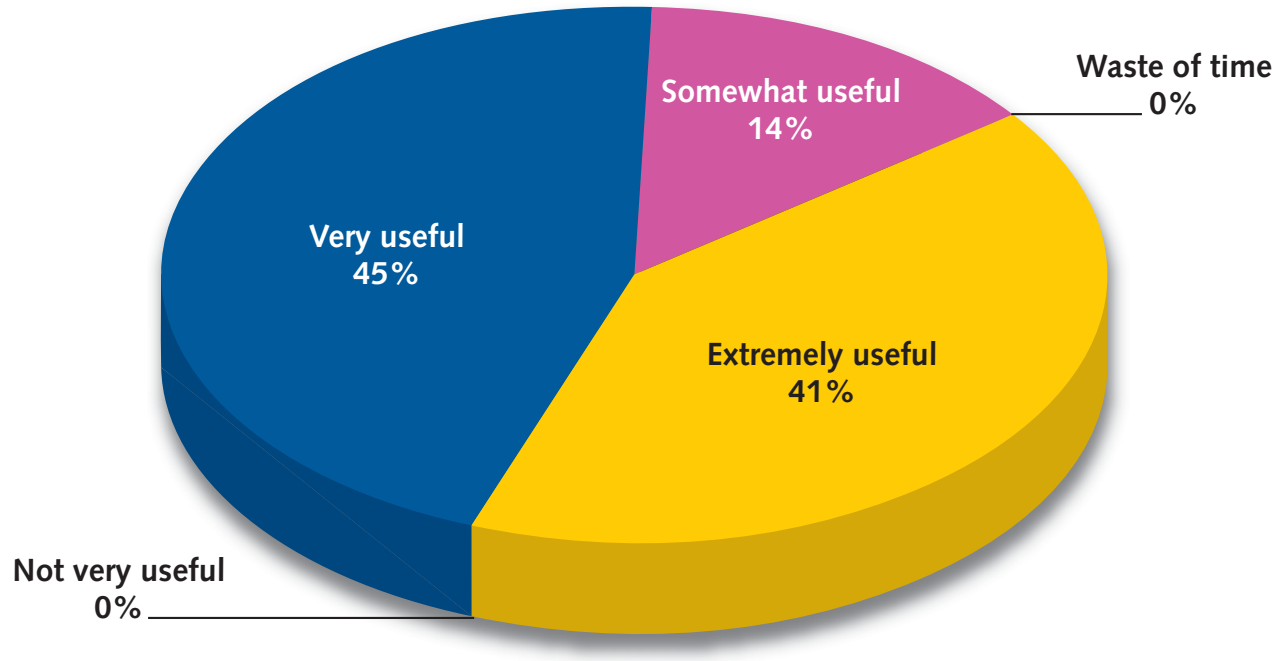


Figure 3: How useful did you perceive the Dry Run to be?

Exercise set-up and pace

The CYBER EUROPE 2010 exercise scenario was structured so that the level of activity varied throughout the day. The activity was at its highest during the first part of the day and slowed down during the afternoon.

In some MS, the CERTs felt that they were overwhelmed, with little time to consider, reflect and act. It is, however, important to remember that different CERTs experienced a different level of activity. It is also important to bear in mind that there are differences between the MS. For example, the scenario escalated to a crisis level at different points in time, due to differences in how MS defined the 'seriousness' of the scenario and also due to differences in structure between states. The fact that the overall crisis management structure looks different between MS is, of course, absolutely normal.

Scenario walk through

The main idea of the first phase of the exercise was to give players the basic information of the scenario, i.e. information that would be shared with the intelligence agencies of MS at a general level during the early stages of an incident. When the players received their first injects, they were asked to try to find relevant contacts in and outside their countries. After 60 minutes, the Exercise Contact Book (ECB) was published. This led the CERTs to create a broadcast list in order to facilitate communication. The initiative to create a broadcast list is actually very close to 'ordinary behaviour' and close to how CERTs usually operate, given their daily role in information sharing. Despite this proximity to their standard operating practices, it was an unexpected development.

The first link went down around 11.15 CET (see Figure 2), which led to a scenario peak between 11.30-12.30. This period was the busiest in terms of scenario injects, since many communication links were supposed to go down. However, by 11.30, players had already given a lot of feedback to their MS-moderators. One could question whether the peak should perhaps have been scheduled for later in the day in order to balance the players' workload and to avoid lunchtime. It is nevertheless important to bear in mind that the exercise was not a drill and hence players were not expected to constantly have injects to react to. The baseline was that the goals of the exercise were to serve as a measurement of success, but not depend on the level of activity being maintained at a constant high. Furthermore, the fact that the pace of activity slowed down towards the end, because people had completed their respective tasks, should be considered as positive.

A map of Europe's Internet Interconnection Sites illustrated the chain of links that went down during the exercise. This map was only visible in the EXCON and each MS was only given a fragment of the map (one map per country). The fact that no playing MS had the entire picture of Europe's IIS, created a difficult task for each MS and stimulated the need for communication. The players acted very cleverly and understood that in order to solve the situation they had to create their own map of Europe, since the problem clearly was not a local one.

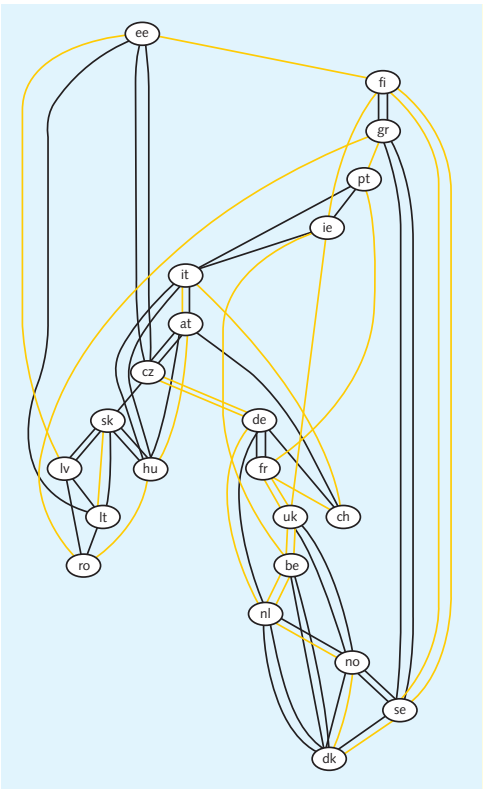


Figure 4: Players map

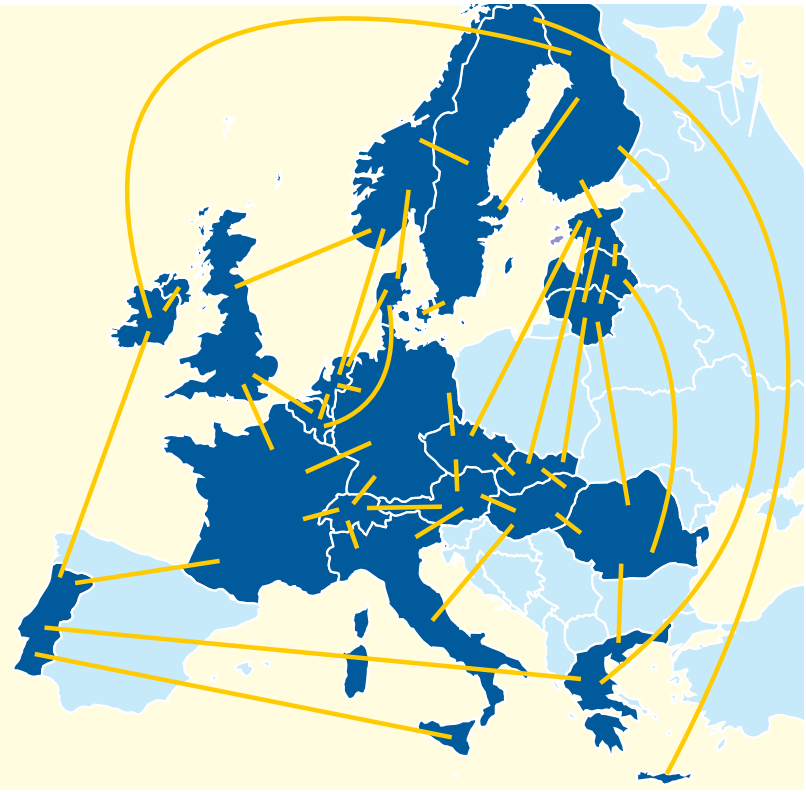


Figure 5: EXCON map

Some of the players felt overloaded during this phase of the exercise, while others were familiar with handling similar situations. The CERTs partly created additional pressure upon themselves due to the fact that they often tried to solve the problem at a level of excessive detail.

At approximately 12.30, an inject announced the upcoming meeting between European Heads of State. The aims of this inject were i) to direct the players within each MS towards the development of a unified external message; and ii) to trigger them to write an official report. This proved to be a very useful task and stimulated those responsible for crisis coordination to draft an easily understandable report, based on information gathered from their CERT community.

Some of the players thought that the afternoon was too calm due to the fact that the pace of injects had decreased. This was, however, not a real problem from an exercise point of view. If the scenario had occurred in real life, the players would also have had to deal with their ordinary tasks. Accordingly, it was important not to create so many different injects that they diminished the 'realism' of the exercise and, additionally, to leave some free time for the players to consolidate their experiences and observations, which were necessary for the exercise evaluation.

From a communications perspective, the exercise can be regarded a success, despite the fact that many players focused more on finding a technical solution to the problem, rather than on the communication with - and flow of information to/from - other participants. Players often requested very detailed technical information, although this could be explained by the fact that the CERTs would generally request this type of information in order to resolve issues at a technical level. It is important to note that the scenario and the injects were built around some challenging technical issues. The fact that the players found ways of solving a problem of such a demanding nature is to be commended.

Figure 6: MS-moderators in discussion

Status reports

Every hour the MS-moderators filled in a status report, covering three main subjects: issues regarding exercise flow, country and connectivity status and the actions taken by the players. The total number of status reports completed by the MS-moderators during the exercise was 190.

20 See: http://www.cpni.gov.uk/Docs/resilience-guide.pdf

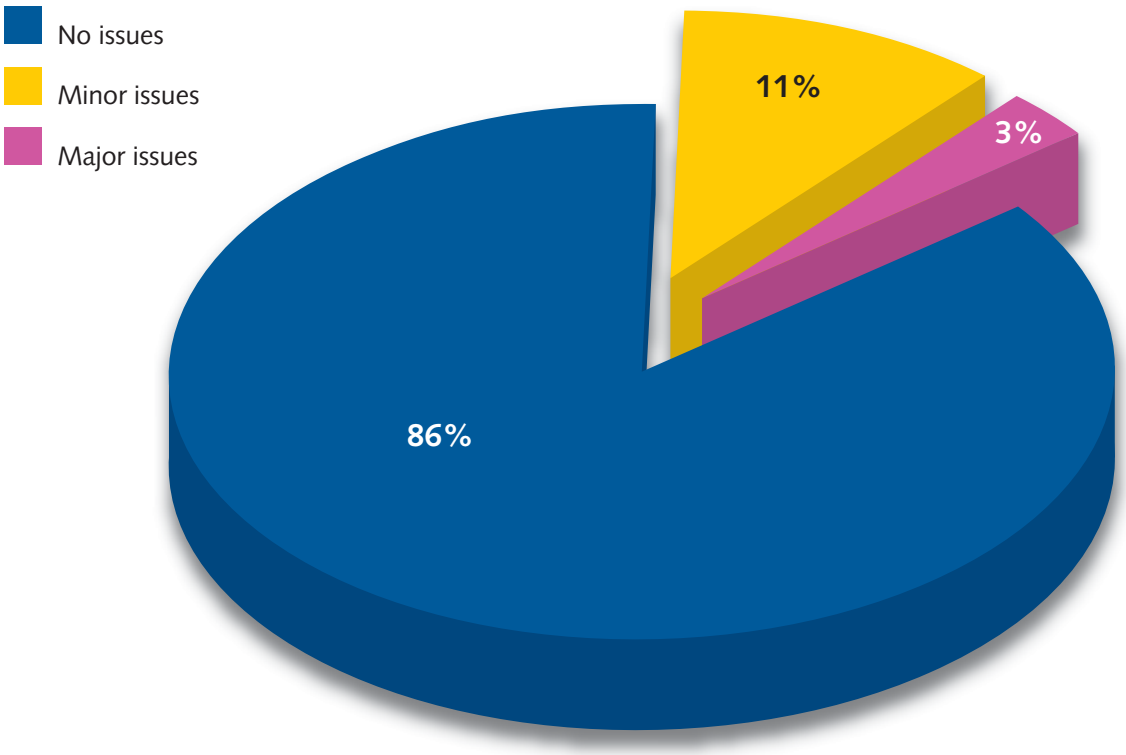


Figure 7: Status reports

For the majority of the time, there were no issues regarding the exercise flow. However, at 10:29 CET, the first minor issue emerged. This consisted of the following:

- Some local real-world issues have emerged in a country that lead to the reduction of the manpower available for the exercise. This should not be a problem, however it showed that real-world issues may influence exercises

During the exercise there were six occasions, according to the status reports, when the MS-moderators reported major issues. These consisted of the following:

- 12:02 CET: major communications links failed. After that event affected countries with connection links direct l ink with MS X had gone down
- 12:07 CET: website defaced "Homepage of the operator X". After that event CERT X called MS-moderator X with question about the existing e-mail lists for all sectorial participants
- 12:22 CET: regarding connection problems between MS X and MS Y, the Agencies in MS X collectively decided that the Internet Service Provider in MS X should deal with this themselves. Also the Agencies in MS X have requested that Agencies in MS Y to respond the same way to the ISP in MS Y. The Agencies should not intervene.
- 12:53 CET: error message received by ENISA.
- 13:03 CET: There was an error in inject "04 Nov 11:49 Incident at IIS": We just had a problem at our IIS3 which connects us to MS X. It was changed to: We just had a problem at our IIS4 which connects us to MS X.
- 15:04 CET: Sometimes we received this as response to my e-mail to exercise-log@enisa.europa.eu: This is an automatically generated Delivery Status Notification.

Four of the six major issues were very closely connected to the exercise play. Only two of the issues, of all the total amount of the status reports, were related to the exercise set-up.

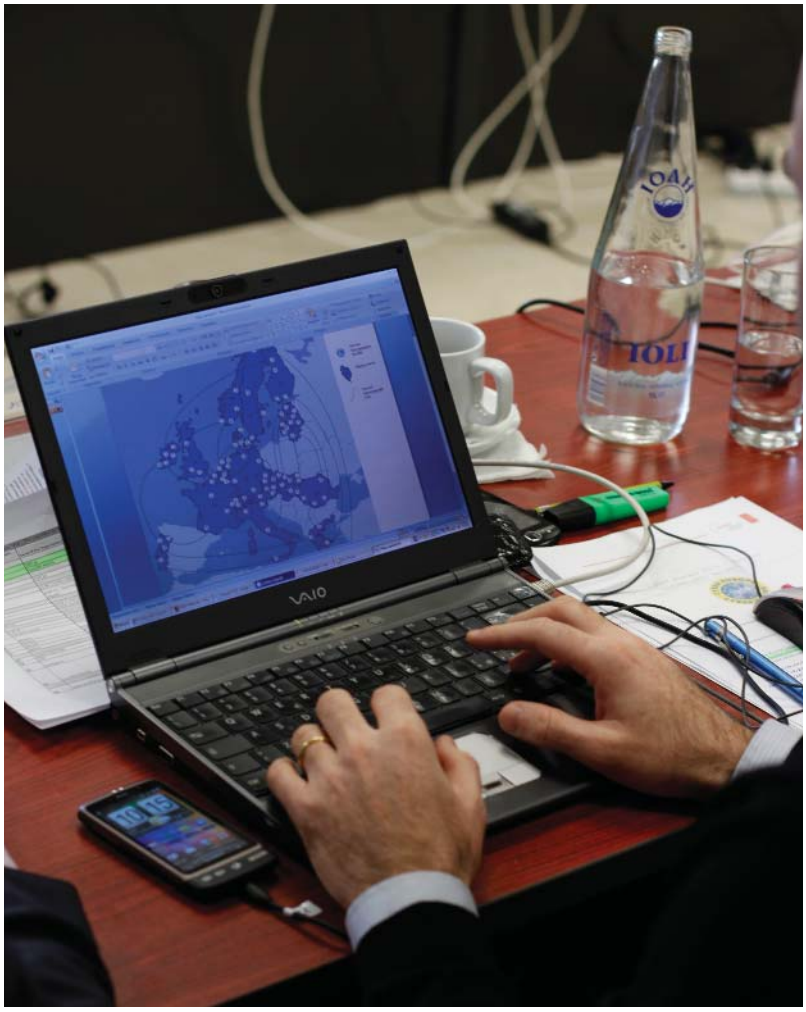


Figure 8: MS-moderator checking national Internet connectivity

Observers group

An observers group was invited to the exercise to study its delivery and execution. The purpose was to give insight into the exercise and its set-up for EU and EFTA MS that did not take part. This was intended to motivate and enable countries to participate in future exercises.

A total of 12 people followed the exercise from a dedicated observers' room, where they had access to the exercise portal containing all injects, status reports and maps. A dedicated exercise narrator was present in the observers' room in order to provide further clarification and guidance. Although a lot of information was given to the observers during the exercise, some felt that it would have been valuable to be part of the whole communication chain between the MS-moderators and their players. The observers group showed a special interest in the national exercise set-up.

Figure 9: Observers group studying the execution of the exercise

Evaluation of the exercise

Evaluation of the exercise

This section is based on the Exercise Debrief session, EXCON-moderators' observations and the outcomes of the individual assessment reports completed by MS.

It was important that the exercise was not regarded as a 'contest' among participating MS.
The evaluation of the exercise was conducted at three levels:

1. National.
2. Pan-European.
3. Evaluation of the exercise itself.

The evaluation of the national part was the sole responsibility of the participating MS. At this level, a self-monitoring approach was undertaken. At the pan-European level of evaluation, the views of the players were presented and summarised in anonymous form. The results at this level were based on the information gathered by the MS-moderators. The purpose of the third level was to ensure the gathering of all lessons learnt for future exercise planning and organisation. At this level, the evaluation focused only on the procedural part of exercise, rather than on the data gathered from it.

During the planning process, two different evaluation forms were developed: i) one version for MS-moderators and, ii) another version for national players. The evaluations form consisted of different questions regarding the main scope and objectives of the CYBER EUROPE 2010 exercise:

The Exercise Debrief was held in Athens on the day after the exercise. The debriefing was divided into three different parts:

1. **General debrief:** what went well, what can be developed and what measures need to be taken?
2. **Reaching the exercise objectives:** to build trust and to increase the understanding among MS about how cyber incidents are handled.
3. **The measures tested during CYBER EUROPE 2010:** the ability to find contact points in the EU and the communication efficiency and the type of data exchanged.

Planning phase

The planning phase of the CYBER EUROPE 2010 exercise benefited from the interaction among the participants, which allowed the interests and concerns of all parties to be taken into account, resulting in a fruitful and highly appreciated exercise. The hard work of the planners group was essential for this success.

Overall, the exercise was perceived as a very well balanced first pan-European exercise and the planning phase served as a good way of helping people to establish and build relationships with each other. The group of people involved was perceived to be small enough to be manageable, while at the same time 'democratically' enabling MS ownership of the overall project. The participating MS thought that it was good that ENISA took the lead. The regular planning conferences were very helpful in guiding and building the exercise structure. ENISA also contributed to this development activity by making all information accessible on the exercise portal. Improvements for the future would be to mark all documentation with date, time, version number and confidentiality type. This would make it clearer and easier to find the right document. The workshops preparing the exercise served their purpose as forums for information exchange between MS.

Future exercises could use pre-exercise conferences for players as a means to create common knowledge and understanding on different themes, or exercise elements. Improvements could also be made by considering/mapping the connection of each MS to others. Each country would benefit greatly from developing this map in advance and a general map could then be distributed to illustrate the 'bigger picture' in terms of interdependencies, connections, links, etc.

Future exercises would also benefit from a longer planning phase, with fixed deadlines and deliverables, allowing the participation of a greater number of countries. It would also be valuable to allow more time for decisions that need to be taken. It is, however, understandable that a rather fast tempo was necessary, due to the fact that the exercise had to be conducted before the end of 2010.

As a result of the relatively short planning phase, the workload placed on the planners group was considered, by some, to be too high. The time pressure also meant that the planning team was limited to eight members. All participating Member States should be members of the planning team. Moreover, for future reference, it would be valuable to have external support from professional companies in place from the start of the planning phase. This is especially important since at times it was hard for the MS involved in the planning phase to internally justify the time they invested in the exercise.

Exercise setting and structure

It was a key success factor that MS-moderators were located at the same premises and were gathered in the same room. The Dry Run was perceived among MS as extremely important in helping to resolve in advance any issues related to exercise technicalities and tools.

During the exercise, there were a few minor technical problems; for example, some injects were delayed or slowed. There were also some minor difficulties with the use of government emails in combination with VPNs. For the future, dedicated exercise hardware, as well as adherence to strict requirements that would be communicated beforehand, could help in eliminating these minor technical problems. Not all moderators were part of the planners group. Since the MS-moderators who participated in the planners group had advance information, they could more easily meet the requests of their countries and handle their players during the exercise, e.g. by giving them dynamic injects to react to. For future exercises, it was suggested by some that the planners group should be widened, with one planner per country assigned to different roles; scenario, media pressure, etc. However, a majority felt that it was much better and more manageable to have smaller groups.

The communication between players did not always work well, for example due to language issues. However, it should be remembered that identifying the level of the communication capability was an explicit exercise objective[3]. Therefore, it was important for the exercise to illustrate what does and does not work properly at the current time. It was good for the observers to be able to follow the exercise, as it helped them to understand their roles as future moderators.

Scenario

The scenario functioned very well and served its purpose in stimulating people to communicate, even if it was on a detailed technical level. The scenario was also perceived to be well balanced between the needs of the more 'technical' players and those consisting of policy makers and Crisis Management Cells. Following the requests of MS to involve a broader group of communities, relevant police and intelligence-focused injects were developed as part of the scenario.

The players reacted to the injects in the 'right' way. The level of activity, all contacts that were established and the overall communication between players was very positive and met the overall goal of the exercise. In addition, the players found solutions and ways of cooperating internationally, even though the main focus of the exercise was not primarily problem solving.

The fact that MS were asked to deliver an official report was very useful and positive from a communications perspective, as the crisis coordination/communications functions had to work on developing a unified and understandable external message.

3 Full details of the players' actions stayed at the national level and are available in the national reports.

During the first phase of the exercise, some MS showed a lack of knowledge about which agency/person was responsible for specific issues/areas. The answers from the players did not always correspond with the contacts in the ECB.

As mentioned earlier, CYBER EUROPE 2010 focused on communication, even though the scenario was of a technical character. The scenario was built to push the players to establish contacts with each other. When it came to law enforcement, the scenario was constructed so that the different national law enforcement agencies had to establish contact with each other. Even though the scenario raised issues at a technical level, solving the puzzle was not the purpose of the exercise.

For future activities, it could be valuable to reflect upon the number of 'target groups' involved, especially when it comes to intelligence. As different groups use different means of communication, for example in order to be able to share classified information, there were certain types/forms of information that could not be distributed during the exercise. This will be especially important to bear in mind when conducting exercises which require a greater degree of problem-solving than the current one.

Although the scenario functioned well, there was an issue during the exercise where the rules of the game were changed by the players. For the future, this could be avoided by making sure that the overall logic and implication of injects (which were the same for all MS) also lead to the same consequences for everyone. In short, the 'translation' of injects into impacts and effects has to be the same for everyone.

The first pan-European exercise could be followed by more complex scenarios, ultimately moving from the European level to a global one. Supporting EU-wide cyber security preparedness exercises is one of the actions foreseen by the Digital Agenda for Europe (see IP/10/581, MEMO/10/199 and MEMO/10/200) to enhance online trust and security.

Objectives

The objectives set for the exercise have been reached. This was highlighted by MS-moderators during the exercise evaluation and in the evaluation forms and this view was also shared by the EXCON-moderators.

To build trust

95% of the MS thought that the exercise was a successful trust building measure (see Figure 10). The objective to build trust was, accordingly, achieved at a general level. The theme of CYBER EUROPE 2010 was communication, and this was borne out during the exercise.

The level of understanding within MS will inevitably vary, depending on the amount of people that are involved in each country. The communication between players helped to increase understanding, but even more so for the MS-moderators who attended pre-exercise workshops in the planning phase.

The fact that one representative (MS-moderator) from each participating MS met and cooperated on a regular basis was probably the most significant trust building measure within the exercise. Players started the process of building trust by establishing connections via e-mail and phone. In many ways, trust between different CERTs already existed, but was enhanced through the exercise.

It is, however, clear that you begin to build trust just by meeting your counterparts, in addition to sharing information and exchanging views.

On a national level, all players learnt something and many were surprised by how well the national teams responded. The scenario could be used as a basis for regional and local exercises.

Some very good initiatives were taken on the national level, for example the players' initiative to discover and draw the European connectivity map (Figure 4), which facilitated the exchange of information.

It is important to remember that the exercise was a first significant step and that more can and should be done, for example by continuing to work on the points of contact that were established during the exercise and by establishing a solid European CIIP-network. The consolidation of trust between MS and partners is a continuing objective. The MS-moderators have now established a good network and probably benefited most from their involvement in the exercise.

MS highlighted that further trust building measures could include the establishment of an information exchange mechanism to promote a culture where information could be easily and quickly shared. Since different groupings may have different objectives, it could also be a good idea to build smaller sub-groups within the area of CIIP. The smaller the groups, the easier it would be to discuss different topics and find solutions to problems.

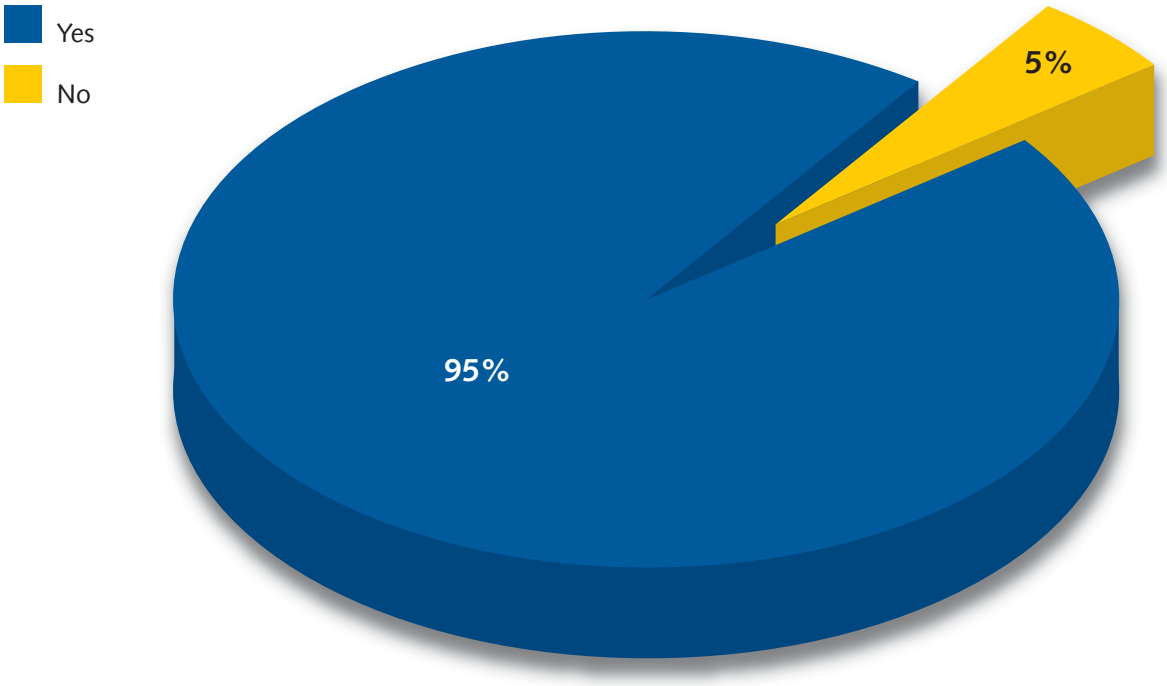


Figure 10: Exercise objective - trust building

To increase the understanding among MS of how cyber incidents are handled

The majority of MS (68%) thought that the exercise increased the understanding of how cyber incidents are handled (see Figure 11). The scenario was built around triggers in order to stimulate communication and to make players establish contacts amongst each other. Communication is a very important factor in the handling of incidents and the fact that communication worked is in itself very positive and a benefit. The interaction between CERTs could serve as a good example. Future exercises could, however, focus on the interaction at a country level and, specifically, between groups that currently are not that used to cooperating on a regular basis.

It is hard to prove that the exercise increased the understanding among MS of how cyber incidents are handled and it is obvious that the artificiality of the scenario to some extent limited the scope of understanding. The exercise has, however, shown that the procedures on how to handle cyber incidents do not yet exist at a pan-European level. Today, cyber incidents are handled at a national level.

MS underlined that it is important to have an agency such as ENISA to provide facilitation services and to organise exercises, in order to further increase the understanding among MS of how cyber incidents are handled.

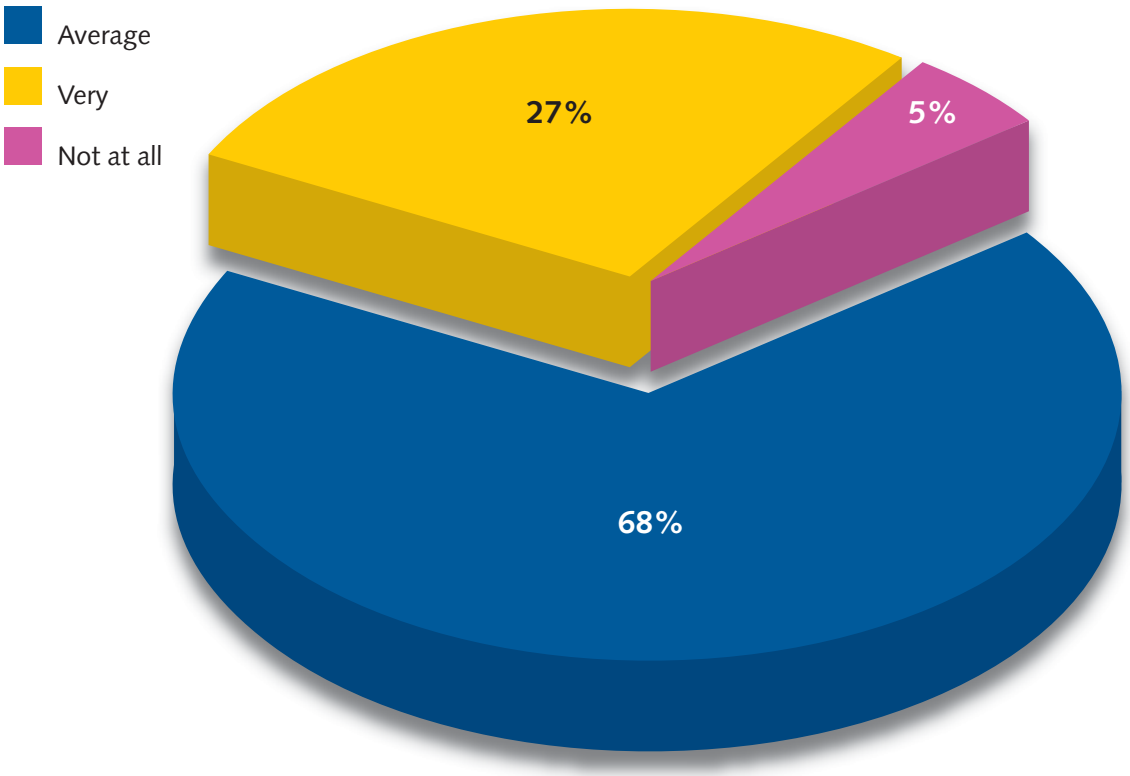


Figure 11: Exercise objective – increase understanding among MS of how cyber incidents are handled

The ability to locate points of contact

The exercise achieved the objectives of testing communication. The communication between players during the exercise enabled a better understanding of how different MS and agencies handle the same issue. Through their participation in the exercise, each MS also recognised that no standard operating procedures exist for the handling of cyber incidents within the EU.

Since each country is organised differently, it is very important that everyone knows who to contact in case of an incident or, more generally, who is able to answer specific questions. In a wider sense, one needs to know who to call in the event of a real incident. The following means were used by the national players in order to find contacts in another country during the exercise:

- ENISA Who is Who
- Meridian CIIP Directory
- Internet search engines
- FIRST directory
- Trusted Introducer lists
- Usual contacts

MS stated that the most important characteristics for defining a valuable directory were that it was:

- Easily available
- Up-to-date
- Clear and structured
- With detailed information

With the available directories, 55% of MS were not at all confident that they would be able to quickly find the right CIIP organisation/s in the appropriate MS, in the event of a real crisis.

MS stated that more exercises would further increase the ability to find relevant points of contact. It could also be useful to keep the directories used in the first part of the exercise (CIIP Meridian, ENISA Who-is-Who) available to Member States through the exercise portal. Updated versions, whenever available, should be accessible via the portal.

All MS were evenly divided in their views on what kind of point of contact would be most appropriate at the EU level; for example, a Single Point of Contact (SPOC) or Multiple Points of Contact (MPOC). Both have advantages and disadvantages. A SPOC would be easier, but today there are multiple points of contact, which is therefore a more realistic option. MPOC also avoids a single point of failure.

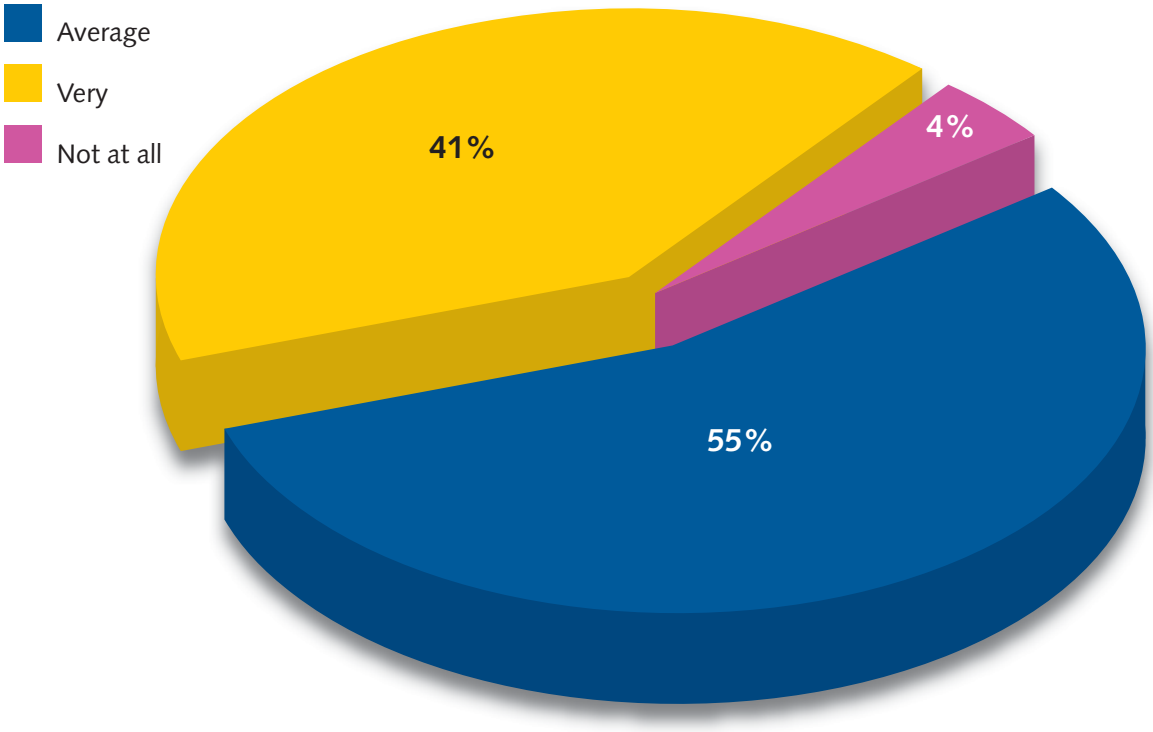


Figure 12: Ability to find contact in a real situation

Efficient communication and data exchange (on a national and European level)

The communications efficiency was perceived as successful, as the exercise led to greater understanding across the EU and illustrated the differences in CIIP structure/s between MS.

The most common difficulties faced by each country's players whilst communicating with other MS were language problems and busy phone lines.

MS underlined that it was important to continue to work on building trust, in order to increase the communication efficiency within the area of CIIP. In addition to taking part in exercises, it is also important to meet face to face in different forums. The better one gets to know one's counterparts, the more efficient the communication will be. The figures overleaf identify the volume of contact between participating MS during the exercise.

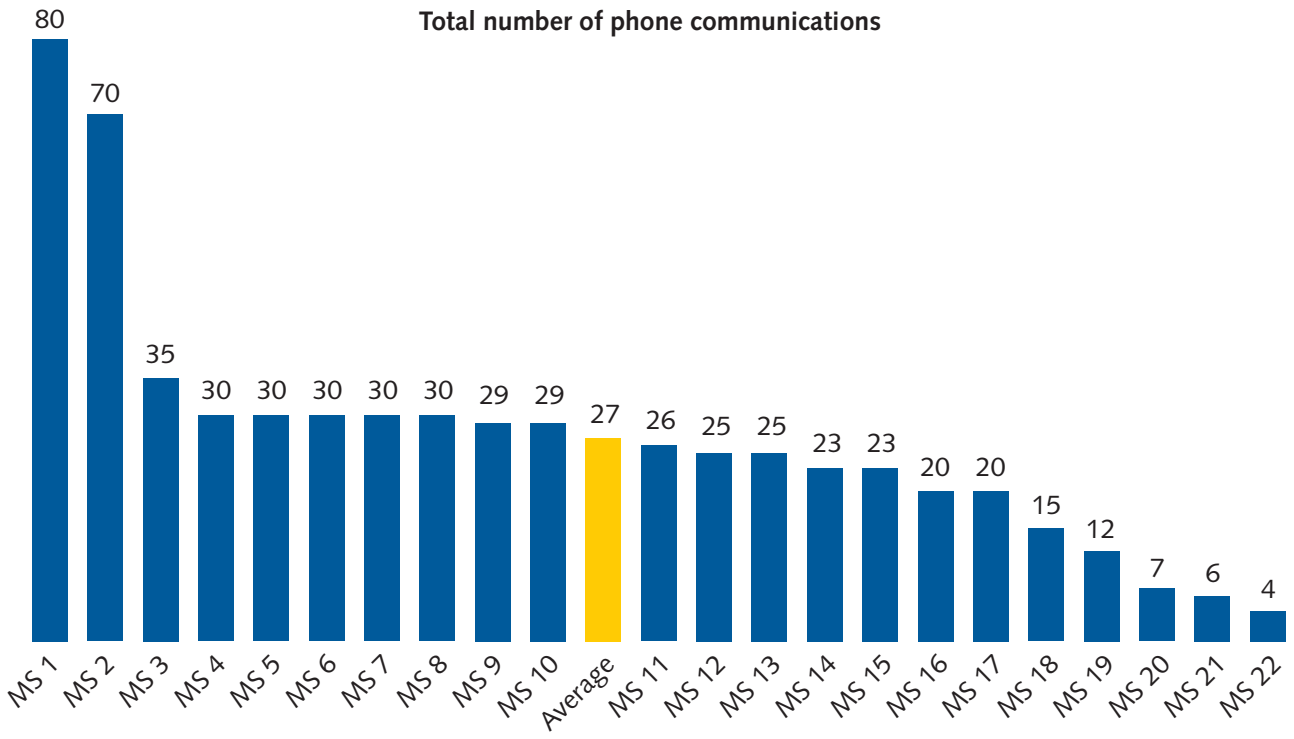


Figure 13: Total number of phone communications

Figure 13 shows that the number of phone calls made by the participating MS ranged from four to 80, with an average of 27.

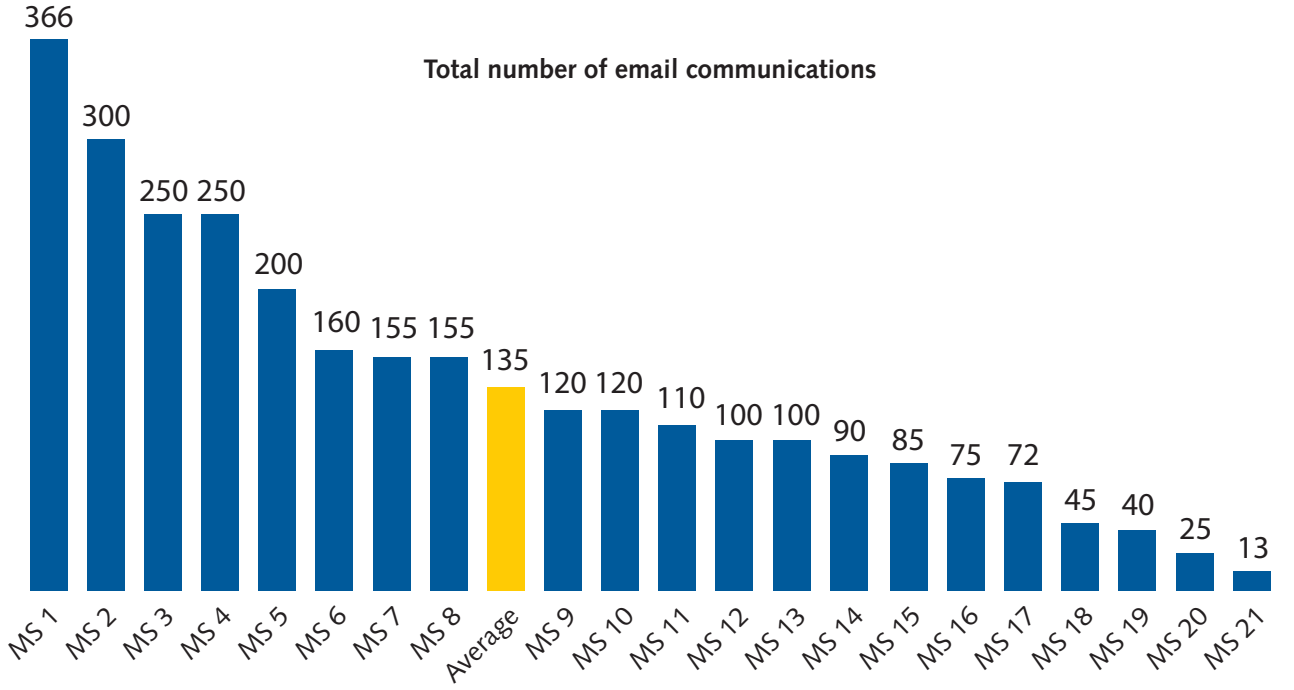


Figure 14: Total number of email communications

Figure 14 shows that the number of emails sent by the participating MS ranged from 13 to 366, with an average of 135[4]. One MS did not count the number of emails (MS 7).

4 MS 7 did not count the number of email communications.

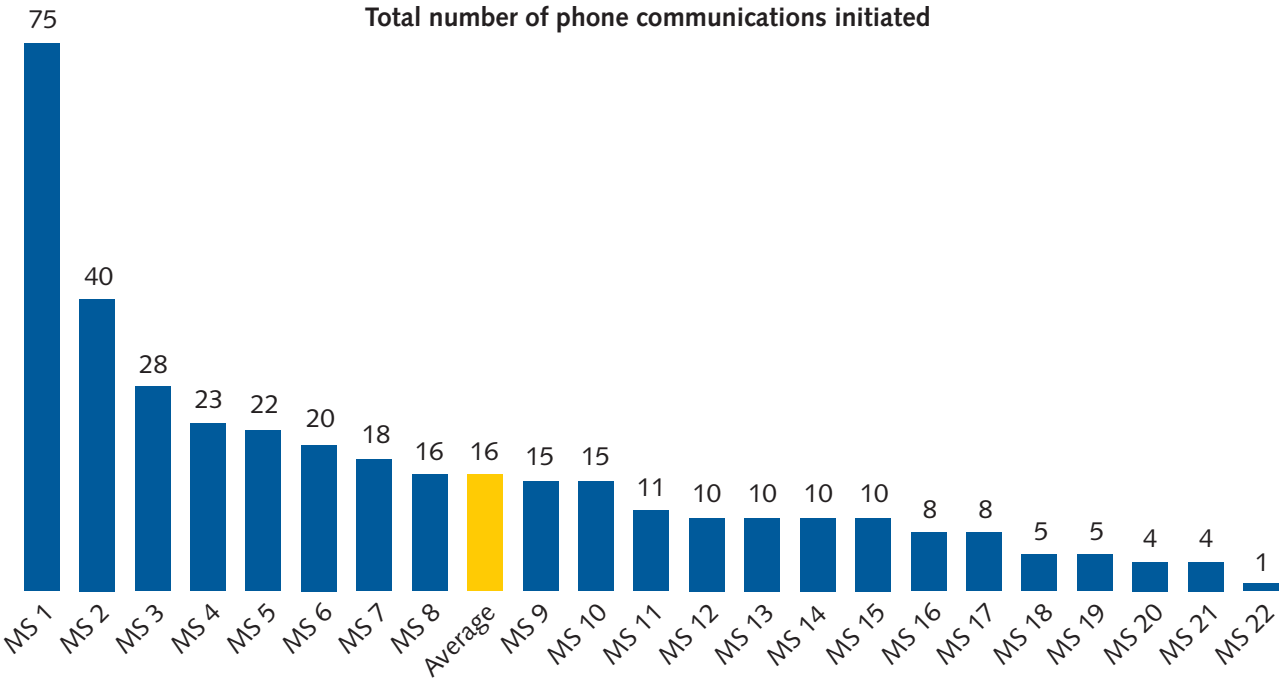


Figure 15: Total number of phone communications initiated

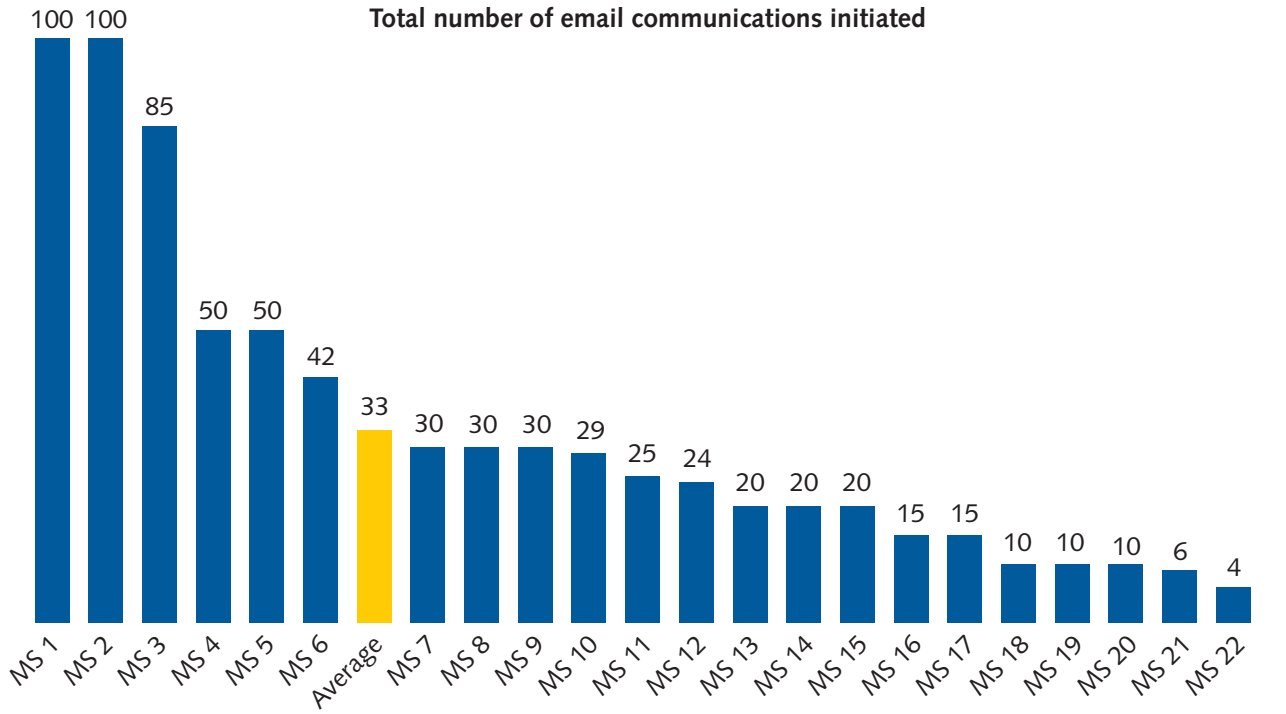


Figure 16: Total number of email communication initiated

Figures 15 and 16 describe the number of times each participating MS initiated contact with another MS. The total number phone calls that were initiated by the participating MS ranged from one to 75, with an average of 16 and the total number of email communication that were initiated ranged from six to 100, with an average of 33.

Additional comments made by participating MS on CYBER EUROPE 2010

- Excellent exercise, we need more of them; build on new, more focused, exercises with more operational issues
- Good occasion for moderators to build trust and learn about national structures
- We are planning to organise our own national exercises and CYBER EUROPE 2010 was a great experience and inspiration for us
- I think that it would be better if the contacts in the ECB were real, because after the exercise this document will not be useful any more

Recommendations and lessons identified

Recommendations and lessons identified

The findings and recommendations of participating Member States of the first pan-European Exercise on CIIP accentuates that CYBER EUROPE 2010 was a useful 'cyber stress test' for Europe's public bodies. MS are very keen to continue their efforts in the area of national and pan-European exercises. ENISA would like to specifically highlight the importance of the following:

- The private sector will provide value in future exercises by increasing the realism (c.f., fictitious infrastructure, scenario)
- Exchange lessons-identified with other (national or international) exercises
- Member States should be well organised internally by, for example, developing national contingency plans, which are maintained and tested on a regular basis through national exercises
- A roadmap for pan-European exercises and preparedness should be created. This will include the definition of standard procedures and structures that should be used in the case of large scale events, such as CYBER EUROPE 2010.

Exercise objectives

To build trust

Recommendations:

- Member States to continue to work on the points of contact that were established during the exercise and to establish a solid European CIIP-network. The consolidation of trust between MS and partners should be a continuing objective
- Member States should continue to organise pan-European exercises in the area of CIIP, because this has proved to be an effective trust building measure
- Future exercises could use 'pre-exercise conferences' for players as a means of creating common knowledge and understanding of different exercise elements. Improvements could also be made by considering/mapping how each Member State is connected to other Member States. Such conferences could be organised at national level by the Member States
- ENISA should help to facilitate the establishment of an information exchange mechanism to promote a culture where information can be easily and quickly shared
- ENISA should help to facilitate the creation of smaller sub-groups within the area of CIIP. Smaller and more focused groups will ease the discussion of specific topics and the identification of solutions to different problems
- Member States should organise debriefing meetings with their players to further facilitate trust building. This could be done back-to-back with other meetings (for example a CERT-meeting), when people are already present.

To increase the understanding among MS of how cyber incidents are handled

Recommendations:

- Member States should continue to organise and participate in pan-European exercises within the area of CIIP, which have proved to be an effective way to increase the understanding among MS of how cyber incidents are handled
- It is important to train the players in advance of the exercises to enhance the learning experience (i.e. national pre-exercise workshops). The exercises should be complemented by conferences and seminars. It is, however, important not to duplicate existing structures and programmes

- More realistic scenarios could have a greater impact on the level of understanding regarding handling of cyber incidents
- Member States should increase their knowledge of how each Member State handles its crisis procedures. Aligning the procedures could be a step towards effective pan-European crisis management
- Information exchange between Member States on how they handle cyber incidents and crisis situations nationally is of paramount importance. Such information exchange could be achieved through dedicated workshops
- The exercise has shown that the procedures on how to handle cyber incidents do not yet exist on a pan-European level. Such procedures need to be identified and tested in future such exercises

To increase the ability to locate points of contact

Recommendations:

- Member States should continue to organise pan-European exercises within the area of CIIP, which has proved to be a good way to locate points of contact
- European countries are organised nationally in a variety of ways. Given the differences in structures and process, it is very important to know who to contact in the case of an incident or, more generally, who is able to answer a specific question
- ENISA should keep the latest versions of the directories that were used in the first part of the exercise (CIIP Meridian, ENISA Who-is-Who) available to Member States through the exercise portal
- The dialogue on the necessity of Single Point of Contact or Multiple Points of Contact on an EU level should continue. ENISA can be the facilitator of this dialogue.

Efficient communication and data exchange (on a national and European level)

Recommendations:

- Trust building measures should continue to be developed as they are closely connected to efficient communication on both national and European levels
- It is important that Member States and agencies are able to meet face to face in different forums (for example during exercises, seminars and conferences). The better the relevant actors get to know their counterparts, the more efficient the communication will be
- The exercise highlighted that Member States communicate in a wide variety of ways. Harmonisation would lead to more secure and efficient communication between Member States. Some form of secure communication would be advisable, for example PGP.

Proposals for future exercises

Member States should continue the dialogue to: i) address topics for future exercises; ii) prepare future scenarios based on more realistic conditions; and iii) create a roadmap for more complex exercises.

The importance of a durable exercise strategy

Because exercises are part of a broader preparedness cycle – which also involves planning, equipment purchases and training activities - multi-year plans should take these issues into consideration.

It is recommended that Member States, with the support of ENISA, draw up a long-term exercise programme, in conjunction with the general strategic planning of their operations. Such an exercise programme should be developed in intensive cooperation between the Member States, in accordance with their priorities, as formulated in ENISA's overall strategy. The exercise programme should cement those priorities by identifying the capabilities that are the most critical to their achievement. An effective exercise programme uses a combination of exercise types to effectively accomplish exercise-specific objectives and programme goals. Such a programme should take into account the national part of the exercise, which should be organised separately by each Member State.

It is, therefore, useful to think of the exercise programme as laying the foundation upon which each building block (i.e. national exercise) builds on the previous one. By adherence to an exercise programme, the relevance and validity of individual simulation exercises can be ensured to a greater extent, with each exercise building on the one preceding it. Such an approach also takes into account the regular turn-over of staff in any one agency, with new employees needing training or simpler drills to be ready to participate in more complex exercises or real events.

It is important, though, that national efforts on exercising do not stop there. Member States are encouraged to organise more, even localised, exercises that will help to increase their level of preparedness.

Also, smaller scale cross country exercises could potentially lead to better cooperation in Europe as a whole.

Planning process

More exercises should be run on national and bilateral bases. In this respect, ENISA will try to help Member States wherever possible. For example, the Good Practice Guide on National Exercises could be utilised.

The nature of the next pan-European exercise on CIIP and its goals should be set before the detailed planning starts. In addition, the players should be informed at an early stage about the estimated time and effort for participation.

Future exercises could use pre-exercise conferences for players as a means to create common knowledge and understanding on different themes/ exercise elements. Improvements could also be made by thinking about considering/mapping the connections between each MS. Furthermore, the Dry Run concept should be included in the planning process of future exercises.

Future exercises would also benefit from a longer planning phase, with fixed deadlines and deliverables. All participating Member States should be members of the planning team. It would also be valuable to assign more time for decisions that need to be taken.

As a result of the relatively short planning phase, the workload put on the planners group was considered - by some - to be too high. More planners could have eased the job of those involved in the planning process. Moreover, for the future, it would be valuable to have a supporting consulting company in place from the beginning of the planning phase. The workload involved in the development and implementation of the exercise set-up to the very last technical detail should not be underestimated. The practical and technical details have a major impact on any exercise execution and just a few problems can undermine the whole organisation effort of an exercise, even in the case of a perfect scenario. This risk should be addressed by long term planning and investment in the development of the appropriate support mechanisms and tools.

Types of future exercise

CYBER EUROPE 2010 was a table top, i.e. a discussion-based exercise, enabling participants to discuss the topics, rather than acting them out. The second pan-European exercise on CIIP could be an exercise that enables the testing of procedures and ensures the preparedness of people to follow them.

There are various options for future exercises. Examples include table top, discussion-based, communication checks, simulations-based, operations-based etc. It is not currently clear if a next pan- European exercise should be table top, or have a more operational character.

Operations-based exercises enable the testing of procedures and ensure preparedness of staff to follow them. These exercises involve acting out the procedures in practice. But as the target of pan- European exercises is to foster *communication* and *collaboration* between countries, a purely operations-based exercise may diminish the importance of cooperation, leading to a competitive environment.

In the long term future, however, and if the main objectives of exercises change, then a distributed operational Command and Post Exercise (CPX) could be an option. Such an exercise strives to create a situation as close to an actual event as possible. This form of exercise is efficient, since it enables practising in stressful situations, which contributes to generating more realistic actions from the exercise players. The degree of verification with this type of exercise is high, but at the same time it is also more complex and demands more comprehensive planning and preparation than a discussion-based table top exercise.

A CPX differs from a table top exercise in three aspects. Firstly, it requires players to respond to each other in the roles assigned to them in the plan. Secondly, it is conducted under time constraints that would be similar to, or often more challenging than, those of a real event. Finally, simulation exercises are usually conducted in the facility designated for coordination and management of a real event, so that all available tools and technologies that would be used in a live situation can be used and evaluated in a controlled and simulated environment. The design, delivery and evaluation of a CPX require considerable resources (internal and external) to ensure maximum effect. Simulation or emulation software might also be used in long term future exercises, in order to increase the realism.

The value of including the private sector

Given the time constraints related to planning and delivery of the first pan-European exercise, it was decided that the private sector would not be involved, in order to keep the level of complexity low. This was considered by all Member States to be a valid approach. However, after the exercise, it was almost unanimously agreed that, in order to achieve more realistic exercises, the private sector must be involved in future. In this way, exercises will have a broader scope and be more realistic, thereby testing measures beyond cross country communication.

One should, however, bear in mind that it is important to start on a small scale, as the exercises will become exponentially more complex as the number of national players increases. One idea could be to start with one private sector representative per Member State and to increase the scope, as each Member State becomes more mature within the area. In addition, standard operating procedures, or other means of coordination, should be discussed and agreed between Member States. Such agreements should also be reflected in relevant policies. The way the private sector is involved in future exercises hence requires additional consideration.

BER EUROPE
2010
BER EUROPE

Appendix

Appendix A – Basic concepts and acronyms

ECB	Exercise Contact Book.
CIIP	Critical Information Infrastructure Protection.
CMC	Crisis Management Cell. The players in one MS, located in the respective country.
CYBER EUROPE 2010	The code name of the pan-European Exercises on issues related to CIIP and large scale incidents.
EFTA	European Free Trade Association.
ENISA	European Network and Information Security Agency.
EXCON	Exercise Control. The exercise headquarters which was in a single central location (Athens), responsible for overall management of the exercise.
EXCON-moderator	Overall exercise moderators located at EXCON, providing assistance to MS-moderators when required.
IIS	Internet Interconnection Sites.
JRC	Joint Research Centre.
MS	Member State.
MS-moderator	Representative from each participating country who managed that country's participation in the exercise. At EXCON, there was at least one MS-moderator to manage each country's participation in the exercise.
Planners	The team that planned CYBER EUROPE 2010 comprising experts from eight Member States (DK, FI, FR, HU, IT, PT, SE, UK), ENISA and JRC.
Players	National agencies participating in the exercise.

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu