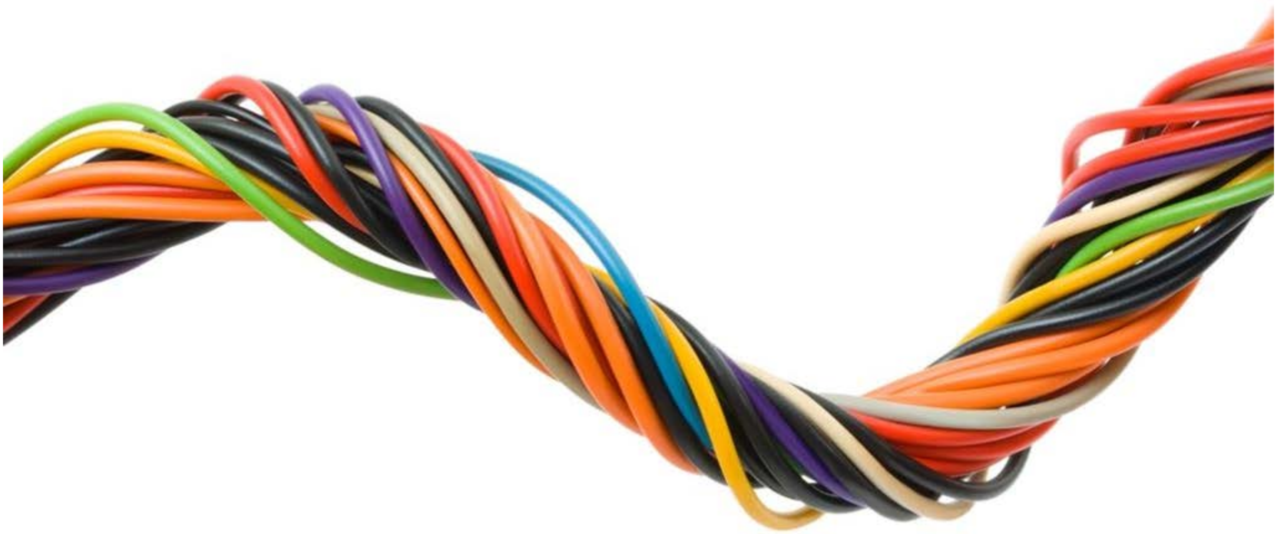
Intended for
ENISA

Document type
Case Study report

Date
September 2015

EVALUATION OF ENISA'S ACTIVITIES
CASE STUDY REPORT – CYBER EUROPE 2014



EVALUATION OF ENISA'S ACTIVITIES
CASE STUDY REPORT – CYBER EUROPE 2014

Revision	**0**
Date	**08/09/2015**
Made by	**VANL**
Checked by	**KARA / HELU**
Approved by	**HELU**
Description	**Case study report – Cyber Europe 2014**

Ramboll
Square de Meeûs 35,
1000 Brussels
Belgium
T +32 (0)2 737 96 80
F +32 (0)2 737 96 99
www.ramboll.com

CONTENTS

TABLE OF FIGURES

TABLE OF BOXES

APPENDICES

1. INTRODUCTION

The following report takes an in-depth and more qualified look at one of ENISA's core operational activities undertaken in 2014, namely Cyber Europe 2014 (CE2014). The rationale for the selection is that the Cyber Exercise is an on-going activity of ENISA with considerable resource allocation. It represents a high profile activity with broad stakeholder involvement from both the public and private sector. It is also an area where follow-up is being made on the basis of the After Action Report that combines quantitative and qualitative data from three sources, namely observations made during the actual exercises, a survey of participants, and two workshops.

The main sources used for the case study are the existing documentation from the follow-up activities, as listed above, and interviews with a sample of seven stakeholders focussing in particular on the operational and strategic level exercises.

The following stakeholder groups were interviewed:

- 5 Moderators / planners, some of whom were also players
- 2 Players[1] –public (no industry representatives were available for interview)

The interview guide for the case study is presented in appendix 1.

[1] An additional three players were contacted for interview, but were unavailable.

2. BACKGROUND

This chapter presents the overall aim of Cyber Europe 2014 (CE 2014), as well as the intervention logic for ENISA's 2014 Work Stream 3 – Support Cooperation, within which CE2014 falls and around which this case study is structured.

2.1 Aim

The goal of CE 2014 was to train European Union and European Free Trade Association Member States (hereafter referred to as Member States) to cooperate during a crisis with cyber components and, more specifically, to assess the effectiveness of cooperation and escalation procedures in the face of cross-border cyber incidents which impact the security of vital services and infrastructure. The exercise also aimed at providing an opportunity for Member States to test their national capabilities, including their level of cybersecurity expertise and national contingency plans, involving both private and public sector entities.

CE2014 had the following key objectives:

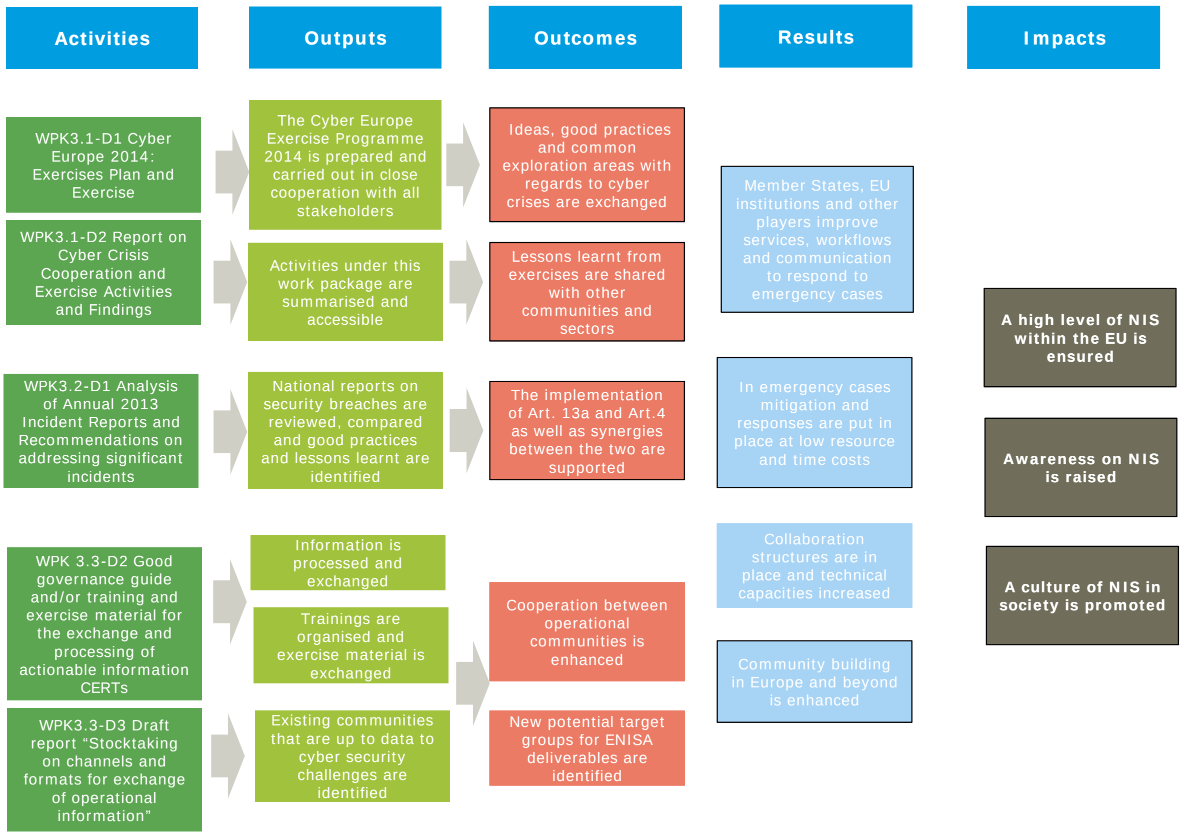
1. Test the European alerting, cooperation and information exchange procedures between national level authorities responsible for cyber incidents
2. Provide an opportunity for Member States to test internally their national Network and Information Security (NIS) contingency plans and capabilities
3. Explore the effect of multiple and parallel information exchanges between private-public and private-private
4. Explore the NIS incident response escalation and de-escalation processes (technical-operational political)
5. Explore the public affairs handling of large-scale cyber incidents

2.2 Intervention logic

The figure below presents the intervention logic for ENISA's 2014 Work Stream 3 – Support Cooperation. This case study focuses on the first activity listed below, namely Cyber Europe 2014 of ENISA's 2014 work package 3.1.

An intervention logic is a systematic and reasoned description of the casual links between the Agency's activities, outputs, outcomes, results and impacts. It helps to understand the objectives of the Agency as a whole and its specific tasks.

Figure 1 Intervention logic for ENISA's 2014 Work Stream 3 – Support Cooperation



Work stream 3 Support Cooperation

The findings presented below have been structured according to the outputs, outcomes and results listed above in relation to CE2014. Making a judgement on to the degree of achievement of the intended outputs, outcomes and results of the exercise enables conclusions to be drawn on the extent to which CE2014 is having an impact on NIS.

3. FINDINGS

This chapter presents the findings from the After Action Report (AAR) of CE2014 and interviews carried out with planners/moderators and players of the exercise. A summative box is included at the end of the sub-sections, compiling the findings in relation to a given output, outcome or result.

3.1 Outputs: Organisation of the exercise

At output level, CE2014 is expected to be prepared and carried out in close collaboration with all stakeholders, in order to ensure that it is relevant and useful for stakeholders.

3.1.1 After Action Report

In accordance with the foreseen output listed in the intervention logic presented above, the CE2014 exercise programme was **organised by ENISA in close cooperation with the participating Member States** through the organisation of six planning conferences held between April 2013 and October 2014. The three exercises which made up CE2014 were interspersed between these planning meetings. In addition, representatives of the EU Council were involved in the organisation of the strategic level exercise.

In order to better address the different layers of cyber crisis management, CE2014 was divided into three escalation phases, spread over 2014 and early 2015: technical, operational and strategic:

- The Technical Level Exercise (TLEx) looked at incident detection, analysis and mitigation, and information exchanges;
- The Operational Level Exercise (OLEx) focussed on alert, cooperation, short-term crisis mitigation, and the creation of a common situation picture;
- The Strategic Level Exercise (SLEx) looked at decision making based on a common situation picture, and high level policy debates on long term crisis mitigation.

Also in line with the expected outputs, the **exercises themselves involved a variety of stakeholders** from the public and private sectors, including technical experts from the public and private CERTs (TLEx), national and/or governmental CERTs (OLEx), representatives of cyber security agencies (TLEx and OLEx), representatives of ministries (OLEx), and representatives of crisis management teams from the private sector, and senior officials responsible for the management of the cybersecurity components pf a crisis within national authorities (SLEx). A number of sectors were also represented, namely the energy (TLEx and OLEx), telecom (TLEx and OLEx), ICT vendor (TLEx), and financial sectors (TLEx), as well as EU institutions (TLEx, OLEx and SLEX).

The AAR suggests that "**pan-European exercises should continue as they are useful**" and that "addressing some of the requirements of EU level NIS policies would be difficult without pan-European exercises". [2]

3.1.2 Interviews

The interviews tended to corroborate the **relevance and usefulness of such exercises**: the exercises were perceived as "absolutely necessary" by one organiser/player in that even though the strategy/plan may not be followed to the letter in a real-life crisis situation, it helps to provide a starting point to the response process. Another stressed the **importance of having the private and public sectors "playing together"** at European level, as private companies tend to be more reluctant to take part and cooperate with national entities. **Interviewees were not able to suggest an alternative actor to ENISA to coordinate such exercises**, stating that it was important to have an actor at European level that could take on this role.The same

[2] AAR: p. 31.

type of exercise would be difficult to organise, for example, by Member States themselves on a rotational basis, as the responsibility to do so would likely rest more with the more experience Member States and would be dependent on their will to do so.

Finally, CE2014 was found by interviewees to **complement other public (and private[3]) interventions**, such as national level cyber exercises which are situated at a different level and have a different focus to CE2014, or the Integrated Political Crisis Response Arrangements (IPCR) exercise at EU level which was a spin-off of CE2014 (see Box 1). In fact, one interviewee stressed the importance of having such exercises at EU level as this meant that private companies had to act as international stakeholders, which would not be possible at national level.

It was also stressed that ENISA could support the organisation of national exercises by providing the tools that they use for planning Cyber Europe, e.g. the incident management guide. Within this context, the AAR makes a general consideration that an increasing amount of cybersecurity exercises are being organised in Europe and around the world, and that there is a growing importance of multilateral and regional alliances, which should be taken into account when planning future exercises, but also in order to promote the exchange of good practices.[4]

The findings presented above from the AAR and interviews point to the fact that C2014 was successfully prepared and carried out in close collaboration with stakeholders from a variety of communities and sectors. Its relevance and usefulness were undisputed and it was perceived as a complementary exercise to other public interventions in particular.

3.2 Outcome: Exchange of ideas, good practices and common exploration areas

At outcome level, CE2014 has a role to play in ensuring that ideas, good practices and common exploration areas with regards to cyber crises are exchanged.

3.2.1 After Action Report

The AAR presents observations, challenges and recommendations in relation to each of the objectives of the exercise on the basis of observations made during the exercise and the feedback gathered thereafter. Drawing on these, and in consultation with Member States, it sets out action points, specifying who the actors are for each and the short, medium and long-term targets for the achievement of these.

3.2.2 Interviews

Interviewees' views were mixed on **whether the CE2014 itself contributed to the sharing of information, ideas and common areas of interest during the actual exercise**, with some perceiving it as an opportunity to do so with players being “open to cooperation” or with “cooperation at CERT level helping to build bridges” and generate new ideas and approaches, and others not perceiving this as one of the objectives of the exercise or seeing room for improvement. One interviewee (TLEx/OLEx player) stated that the exercise was not about sharing information, but about assessing the technical level and resolve problems (TLEx) and improving the ability to react to an incident (OLEx); this was in part done through testing the channels and means employed to exchange information. Another interviewee stressed that “in an exercise everyone shares everything” as it is the key point of the exercise, but expressed doubts as to the extent such a degree of information would be shared “in real life” as there is always the risk that the information will not be judged important by the recipient and of overloading the recipient with information that proves a challenge to summarise and prioritise.
This view stands in contrast to that expressed by another player who found that during the exercise the interaction between Member States “did not pick up” and that most tried to solve

[3] Unfortunately it was not possible to interview a private sector representative to seek their views on this point.
[4] AAR: p. 31.

the problem by interacting with those they normally interact with in day-to-day situations, only reaching out to others at some points, but not following up with them to the same extent. The reasons given for this were the low level of maturity of the implementation of EU-Standard Operating Procedures (EU-SOPs) and lack of knowledge about participants' capacity.

When asked **whether the sharing of information, ideas and common areas of interest continues after an exercise has ended**, interviewees were generally of the opinion that CE2014 contacts are maintained to some extent, but that established contacts tend to be those most solicited. One interviewee stated that the exercise itself was "the key moment for exchange", while another said that there was a "discrepancy between the exercises and real life" as in real life people will tend to use their established bilateral connections to first check whether an incident is severe enough to share it via SOPs. A further interviewee concurred, stating that "the challenge for ENISA is to establish a mechanism that does not only work in the exercise, but also in real life". A recommendation was made in this respect that an information sharing platform be established as a more formal structure to exchange views on more day-to-day incidents, helping to judge their severity, exchange solutions etc.; such platforms exist at European level for example in the financial sector. The NIS Directive was seen as an opportunity to establish such a structure.

Furthermore, the preparation workshops for CE2014 were referred to by a couple of interviewees as a good means to exchange information and learn, e.g. about the state of preparedness of given Member States and the differences between Member States such as in relation the existence or not of systems for secure communication. In another instance, reference was also made to the post-exercise workshops aimed at exchanging conclusions among participants.

The box below presents details of a **spin-off of CE2014**, illustrating a further way in which the exercises can add value through a broader exchange of ideas.

Box 1 Exercise for the integrated political crisis response arrangements (ICPR)

A first exercise within the framework of the new set of Integrated Political Crisis Response Arrangements (ICPR)[5] was organised in November 2014 with the aim of testing and validating the draft SOPs which had not been fully agreed at the time. As CE2014 included a strategic phase, it was used as a spin-off for the IPCR-related exercise. As a first ICPR exercise, the level of ambition needed to be moderated which, along with the specificities of the community they were dealing with, is why it was not connected directly to CE2014 in the form of the SLEx. However, the storyline of CE2014 was used as a trigger for the ICPR exercise which focussed on consequence management in a situation where critical infrastructures are affected and a trans-boundary (geographical and sectorial) crisis is reached. The EU Council was able to use the storyline and parts of the videos and material developed by ENISA for the SLEx, rather than start from scratch and work in isolation. This helped the EU Council save time and resources, providing important added value. ENISA assisted in the planning and participated in the exercise itself, providing their views as the subject matter experts on cyber security, which was the trigger of the exercise. The cooperation between the EU Council and ENISA in the planning of the exercise, and the fact that ENISA took part in the exercise itself, according to the interviewee, brought more visibility to what ENISA is doing at EU Council level, and raised awareness about cyber threats more generally among participants.

Finally, it is worthy of note that the interviews revealed that **work had begun on a number of the short-term action points set out in the AAR** (see Appendix 1 for more details), with the involvement of some of those interviewed. Most notably, reference was made to the work being carried out by a dedicated team on the short-team actions relating to the EU-SOPs (i.e. A9 to A16 on establishing a formal editorial team, developing written procedures for the development of EU-SOPs, establishing an update plan and adopting a consensual yet flexible approval process for the EU-SOPs). In addition, a working group was said to be looking into gathering requirements from Member States for a cooperation platform (i.e. A20), which is an action point related to the NIS Directive.

The findings presented above from the AAR and interviews point to the fact that C2014 facilitated the exchange of ideas, good practices and common exploration areas with regards to cyber crises through its preparatory phases, the exercise itself, the AAR, the ICPR spin-off and the (short-term) action points set out in the AAR, but that there is a discrepancy between the exercises and real life as in real life people will favour established contacts over news ones, for example in order to first check whether an incident is severe enough to share it via SOPs. It was recommended that an information sharing platform be established (via the NIS Directive) as a more formal structure to exchange views more regularly on more day-to-day incidents.

3.3 Outcome: Sharing of lessons learnt

At outcome level, CE2014 has a role to play in ensuring lessons learned are shared with other communities and sectors.

3.3.1 After Action Report

As in the case of the exchange of ideas, good practices and common exploration areas discussed above (see section 3.2.1), the AAR in itself – and exercise observation, post-action surveys and workshops which form the basis of it - is a means of sharing lessons learnt.

[5] The EU Integrated Political Crisis Response arrangements (IPCR) reinforce the European Union's ability to take rapid decisions when facing major crises requiring a response at EU political level. They were approved on 25 June 2013 by the Council of the European Union. http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

3.3.2 Interviews

A couple of interviewees referred to national-level **post-exercise debriefing meetings** organised among participants in order **to discuss the principal achievements of the exercise and draw out lessons learned**. One interviewee stressed that not all lesson learned can be shared with everybody and that each one should be assessed individually and an action plan and actor(s) established in relation to it.

The interviews suggest that lessons learned (e.g. in the form of the ARR itself) **tend to be shared within a "semi-closed" circle of interested parties**, often within national administrations/the organisations concerned in particular. In one instance reference was made to a cyber-security coalition between private partners, academia and the government in which lessons are shared, while in another an event was organised with all players and additional stakeholders to share lessons learned and build awareness of the exercise in order to seek to involve more players in future exercises.

Finally, in one instance, lessons learned were said to be **disseminated to the political level** and a further interviewee suggested that it could be helpful to disseminate at the governmental level the results of the exercise in order to increase awareness among decision-makers as in the case of major incidents, the ability to engage the decision makers is fundamental.

The **wider dissemination of lessons learned is often not to be favoured** due to the sensitivity of the topic area, e.g. the exercise may point to vulnerabilities in the public or private sector, and the lessons are relevant to a specific community / target audience and not others. That said, information on the fact that such exercises are being prepared and conducted could be addressed to a larger public to show that preparations are in place to deal with a potential crisis.

The findings presented above from the AAR and interviews suggest that the lessons learned from C2014 are being shared through the AAR and national-level post-exercise debriefing sessions, with in some instances these sessions being broadened to include people other than exercise participants. Lessons learned tend to be shared within a semi-closed circle of interested parties or disseminated to higher political levels due to the sensitivity of the information, which acts as a legitimate barrier to wider dissemination.

3.4 Outcome: Cooperation between operational communities

At output level, ENISA seeks to enhance cooperation between operational communities; the degree to which CE2014 has contributed to this is assessed below.

3.4.1 Post-exercise surveys

The post-OLEx exercise survey looked to establish the degree of cooperation over the course of the exercise between the different actors. In a number of cases, the highest proportion of respondents (representing between 30% and 45%) stated that they had not cooperated with the named actor. This was the case for the energy sector and ministries (40%); ISP/Telco and cyber security agencies (33%); ISP/Telco and ministries/e-government agencies (45%); and ministries/e-government agencies and cyber security agencies (31%). Higher levels of cooperation took place among ISP/Telco and the energy sector and the energy sector and cyber security agencies.

Furthermore, the results of the post-exercise surveys suggest that:

- More than half of the participants in OLEx were satisfied with international cooperation, but more than one third felt that it could be improved.
- European cooperation at strategic level during a crisis was regarded positively by the large majority of Member States, e.g., 18 out of 20 in SLEx.

3.4.2 After Action Report

The AAR stresses that "**a lack of certain levels of trust**" between Member States acted as a barrier to efficient cooperation during cyber incidents and even more so during crisis situations.

The AAR further suggests that the objective of the exercise which aimed to "test the European alerting, cooperation and information exchange procedures between national-level authorities responsible for cyber incidents" was only partially achieved as **opportunities for cooperation at multinational level** were not provided and the artificial separation of TLEx and OLEx reduced opportunities for cooperation. It was recommended that future Cyber Europe Exercises "continue to provide opportunities to test bilateral and multilateral cooperation at technical, operational and strategic levels, taking into account existing clustering arrangements".

Moreover, the third objective of the exercise which seeks to **explore public and private cooperation**, and in particular "the effect of multiple and parallel information exchanges between private-public and private-private", was not met in that the exercise did not monitor such exchanges and Member States did not provide evidence on the effects of such exchanges.

Finally, CE2014 aimed through both OLEx and SLEx to "**explore the public affairs handling of large-scale cyber incidents**". This objective was partially met through OLEx including injects relating to public affairs that allowed for the exploration of this dimension, but only few Member States involved public affairs experts during OLEx and reported on such activity, and no directory of such experts was included in the exercise. During the SLEX, the importance of this dimension was discussed.

3.4.3 Interviews

Interviewees were asked **whether they cooperate (more) with other operational communities** with regard to emergency and/or threats than they did prior to the exercise, and whether this increased cooperation was a result of the exercise. **Views were mixed** in this respect with one interviewee stating that cooperation has increased as "it generally improves cooperation to know people in person" and the exercise being perceived as a good means not just to create new relationships, but to strengthen existing ones (e.g. among CERTs). On the other hand, cooperation with other operational communities was said to be "in place" or "existing" (e.g. between Member States through the establishment of working groups, through bilateral engagements), but was qualified as "not very close" with limited interface between governmental and private companies' procedures in one instance or "not the result of the exercise itself" in another two.

One interviewee stressed that the degree to which the exercise leads to increased cooperation will depend on what happens after it, i.e. whether there is an incident involving the country with the new contact point, as "there is a long way to go" between knowing of the existence of a new contact point and having a good exchange of information with that contact. As a result, it was suggested that it may make sense to have more regular communication checks outside the two-yearly exercises in order to "lower the barriers", encourage people to get in contact and check their contacts.

The findings presented above from the post-exercise surveys, AAR and interviews point to the fact that C2014 has enhanced cooperation between operational communities to a relatively limited extent as this is a long-term process which involves the building of trust. During the exercises themselves, a number of actors did not cooperate with each other / across the public-private divide, few Member States involved public affairs experts, and opportunities for cooperation at multinational level were not provided. Moreover, cooperation levels with other communities post-exercise seem to remain the same – though with existing relationships having been strengthened. Where such cooperation levels do increase post-exercise, this can be dependent on whether an incident provides a reason to cooperate with a new contact / different operational community. Within this context, it was recommended that ENISA organise more regular communication checks outside the two-yearly exercises in order to "lower the barriers", encourage people to get in contact and check their contacts.

3.5 Result: Improvements to services, workflows and communication

ENISA aims to ensure at result level that Member States, EU institutions and other players improve their services, workflows and communication to respond to emergency cases.

3.5.1 After Action Report

The CE2014 exercise provided the opportunity for Member States to "test internally their **national NIS contingency plans and capabilities**". The AAR report suggests that this objective of the exercise was met in that:

- "Most Member States tested their incident handling procedures and capabilities during TLEx."
- "Most Member States tested their national-level crisis management procedures and capabilities during OLEx."
- "SLEx was an opportunity to raise awareness on national contingency plans."

Moreover, the fourth objective of CE2014 which sought "to explore the NIS incident response **escalation and de-escalation processes** (technical, operational and political)" was found to have been partially met with challenges to its achievement including limited cooperation during TLEx, time and resources constraints which prevented the drafting of a Common Operational Picture (COP) during OLEx, a lack of continuity between the three phases of CE2014, etc.

The AAR further suggests that the OLEx exercise enabled EU-SOPs to be tested "to a large extent as participants used them to **alert each other, exchange information** and create a common operational picture". However, despite several Member States having discovered the true origin of the attack, failure to share the information on a multilateral level resulted in most Member States not having the information.

Moreover, CE2014 revealed that existing **means of secure communication** identified in the EU-SOPs were not efficient and did not facilitate the process of information sharing during the drafting of the COP. Despite different platforms having been used during OLEx, more than half of actors think that it would – or may be – useful to develop a platform for supporting cooperation on EU-SOPs.

3.5.2 Interviews

Interviewees were asked **whether the exercises improved work processes (speed of processing) and communication (information sharing) to respond to crises**; the majority felt that it had done so, in particular at national level.

Those who felt this was the case referred more generally to the fact that the exercises improved work processes and communication because: they enabled them to be tested and see what works and what does not; multiple players were involved from given national settings; or the exercises helped show what parts of a normal crisis approach, applicable in other sectors, needed to be adapted to cyber incidents, which are much faster in pace. In more concrete terms, further to the exercise and weaknesses it exposed, one Member State decided to define a list of participants' public keys in order to be able to reach multiple destinations with just one e-mail. A further interviewee stated that the exercises had helped set up an EU cyber prevention plan at national level, and identify weaknesses and put in place new procedures in response to these.

However, it was further stressed that **it cannot be said that an EU-level crisis management process has been put in place as a result of the exercise**; there is still not sufficient response at the EU level. This view was shared by an interviewee who stated that the exercises showed weaknesses in terms of secure communication for information sharing among given players at EU level, rather than providing solutions.

Recommendations to improve the exercises in order to lead to further changes in relation to work processes and communication included, at EU level, first ensuring a common understanding and documented procedure and then, ensuring it is implemented by Member States and other organisations. In addition, reference was made to the creation of a platform for lower level, day-to-day communications, as referred to above (see section 3.2.2). It was also recommended that the exercise be “played to the end”, to the strategic level over a longer, less intense three-day period.

Moreover, the importance of holding the exercises on a regular basis (every 2 years) was stressed within this context, as was continuing to define specific scenarios and looking to involve other sectors in the exercises. It was also suggested that having multiple storylines that countries could choose from unnecessarily complicated the CE2014 exercise.

When asked **whether the exercises contributed to identifying gaps in their technical capacity to respond to a crisis situation**, a few interviewees said the TLEx in particular will have done so, but in a number of cases they were not party to this exercise. In one instance, it was said that no technical gaps were identified with the technical teams having worked “very well”, and that the main problems identified concerned communication.

The findings presented above from the AAR and interviews suggest that C2014 has led to improvements in Member States’ services, workflows and communication to respond to emergency cases at national level in that they allowed for national NIS contingency plans and capabilities to be tested and technical gaps to be identified, where relevant, and led to concrete action being taken at national level in relation to any weaknesses identified.

The exercises also served to identify weaknesses in the level of alerts and exchanges of information, and the level of secure means with which to so do, suggesting that there is still a long road ahead before an EU-level crisis management process is put in place.

3.6 Result: Emergency cases, mitigation and responses

At the level of results, ENISA aims to ensure that in emergency cases, mitigation and responses are put in place at low resource and time costs.

3.6.1 After Action Report

The European Standard Operations Procedures (EU-SOPs), which aim to improve information exchange and cooperation at operational level between Member States in order to elaborate a common operational picture for upper crisis management layers to understand and mitigate the crisis, are a key element of the EU-level mitigation of and response to cyber crises. According to the AAR, exercise participants have not actually made use of the EU-SOPs[6] as no large-scale cyber security incidents have justified their use since their introduction in 2010. However, the majority of players stated in the OLEx post-exercise evaluation questionnaire that **EU-SOPs are**

---

[6] The European Standard Operations Procedures (EU-SOPs), part of a wider cooperation framework called the European Cyber Crisis Cooperation Framework (ECCCF), were developed to be used by the operational coordination bodies from public authorities in all Member States, when involved in the management of multinational cyber crises. The objective of the EU-SOPs is to improve information exchange and cooperation at operational level between Member States in order to elaborate a common operational picture for upper crisis management layers to understand and mitigate the crisis. The EU-SOPs were designed by and for Member States through support from ENISA and with input from willing contributors; in the future, a formal editorial team made up of Member States will be re-introduction (not active for CE2014) as ENISA alone cannot bear the responsibility of the development of EU-SOPs.

useful, added clarity and helped achieve situational awareness.[7] Overall, participants identified the need to further pursue the development of the EU-SOPs in order to enable the management of cyber security incidents, and the need to practice using EU-SOPs to ensure their use should such an incident occur.

While the exercise was seen as a good opportunity to test and improve cybersecurity capabilities, it was acknowledged that **national capabilities need to be further built up in order to ensure the effective management of large-scale cyber incidents at the European level**. ENISA has consequently been tasked on the mid to long-term with supporting the maintenance of cybersecurity expertise through offering technical cybersecurity and operational crisis management trainings on a regular basis, and organise regular exercises offering Member States the possibility to assess their NIS capabilities.[8]

3.6.2 Interviews

Interviewees were asked **whether the exercises supported the development of mitigation and response strategies**. At the national level, a few interviewees stated that this was not the case as their national strategies / response plans were already in place at the time of the exercise. The exercises were said to have "helped formalise those mitigation and response strategies that were applied". In one instance, it was said that the lessons learned from CE2014 could be used to define contingency plans that were in the development stage at the time of writing.

At European level, it was stated that the development of such mitigation and response strategies takes time – there has been progress made, but there is still work needed.

Overall, interviewees found it difficult to comment on **the degree to which ENISA contributes to putting in place cost effective procedures and mitigation and response strategies**, and provide ideas of more or less costly alternatives. One interviewee stated that having the exercises and EU-SOPs is simply something that has to be done; he could not identify any other opportunities / alternatives. In another instance, it was stated that it was helpful to be able to use at national level some of the things learned during the exercises, e.g. in relation to speeding up the information exchange by knowing what information to send to whom, identify and test means to approach / talk to the private sector.

When asked **whether they had ever applied to real incidents the experiences gained in mitigation and response through the exercises**, it was stressed that fortunately no such large-scale cyber crisis had affected Europe since the inception of the Cyber Exercises. However, in two instances, reference was made to the fact that **internal processes and incident procedures were adapted as a consequence of the exercises**. In more concrete terms, a further interviewee referred to the fact that the lessons learned in relation to alerting and information exchange in particular had been applied to real incidents, e.g. ensuring the correct numbers are used for given incidents and further testing these with non-participants, ensuring awareness of the availability of a given unit for whom contact details are made available.

The findings presented above from the AAR and interviews point to the fact that C2014 is working towards ensuring that in emergency cases, mitigation and responses are put in place (at low resources and time costs), by providing a good opportunity to test and improve cybersecurity capabilities and take action at national level in relation to any lessons learned. However, the need has not yet arisen to make use of EU-SOPs and national capabilities need to be further built up in order to ensure the effective management of large-scale cyber incidents at the European level.

[7] AAR: p.21
[8] AAR: p. 29, 39

3.7 Result: Community building in Europe and beyond

At result level, ENISA seeks to enhance community building in Europe and beyond; the findings presented below seek to ascertain the extent to which CE2014 has helped it do so.

3.7.1 After Action Report

The AAR suggests that one of the achievements of CE2014 was the fact that it raised awareness within given communities, with several OLEx participants from the energy sector welcoming the opportunity provided by the exercise to do so within their sector.[9]

3.7.2 Interviews

The **planning and execution of CE2014 were seen by interviewees as a means to contribute to community building in Europe and beyond**. People tend to work more with their own community of expertise and in relation to a certain sector at national, local or institutional level, so "running and playing an exercise with many different Member States and institutions helps build that community".

The **planning** of CE2014 was seen by the majority of interviewees as playing a key role in this community building. One interviewee suggested that the planning that goes into CE2014 is perhaps more important than the exercise itself in doing this as it involves needing to plan and coordinate with others, creating informal structures, gaining insights into each other's work and building trust. A further interviewee concurred, stating that "the planning process of the exercise itself offers a new interaction and interface with others that we do not normally interact with". It was also stated that "a first advantage of organising the exercise is that a community of planners has been created".

The **exercise itself** was also perceived as a good opportunity to test existing relationships and see how they could be improved. It was stated that "it is a lot easier to pick up the phone when you know the people on the other end". In particular, "a strong community" was said to have been built up in particular between those that participate in each exercise; some Member States rotate their staff for different versions of the exercise, while others send the same participants which allows for more community building.

The findings presented above from the AAR and interviews point to the fact that C2014 has contributed to community building, both through the preparation and implementation of the exercise, and raising awareness.

[9] AAR, p.29

4. CONCLUSIONS

In order to ascertain the effectiveness of CE2014, it is first essential to establish whether it reached its stated objectives at output, outcome and result level. On the basis of the findings presented in the preceding chapter, it can be concluded that:

- At output level, ENISA achieved its objectives in that the CE2014 programme was prepared and carried out in close collaboration with a variety of stakeholders. Those interviewed stressed the relevance and usefulness of the exercises and essential role that ENISA plays in their organisation and coordination.
- At the outcome level, the CE2014 exercise facilitated the exchange of ideas, good practices and common exploration areas, and the sharing of lessons learned among communities and sectors to a certain extent, but that there is a discrepancy between the exercises and real life as in real life people will favour established contacts over news ones.
- At the outcome and result level, despite issues of a lack of trust and a tendency to continue contacting established contacts after an exercise has been carried out, the planning and implementation of the exercises facilitate cooperation between operational communities, and one of the exercises' key achievements is their contribution to enhancing community building in Europe and beyond. As one interviewee put it, "even if we don't call every day, we met, exchanged things, and worked together, so CE2014 did contribute to building a community of crisis managers".
- At the result level, C2014 has led to improvements in Member States' services, workflows and communication to respond to emergency cases at national level in that it allowed for national NIS contingency plans and capabilities to be tested and technical gaps to be identified, where relevant, and led to concrete action being taken at national level in relation to any weaknesses identified. However, there is still a long road ahead before an EU-level crisis management process is put in place.
- At the result level, C2014 is working towards ensuring that in emergency cases, mitigation and responses are put in place (at low resources and time costs), by providing a good opportunity to test and improve cybersecurity capabilities and take action at national level in relation to any lessons learned. However, national capabilities need to be further built up in order to ensure the effective management of large-scale cyber incidents at the European level.

The degree to which the CE2014 exercise has met its objectives at output, outcome and result level can, in turn, enable some tentative conclusions to be drawn in relation to the impact it has had in terms of ensuring a high level of NIS in the EU, raising awareness of NIS and promoting a culture of NIS in society, as detailed below.

The conclusions above suggest that CE2014, in bringing together representatives of different communities and sectors - both public and private - to cooperate and test national response capacities in the event of a trans-boundary cyber crisis, is **working towards ensuring a high level of NIS in the EU** and increasing awareness of it. As one interviewee put it, "the great advantage of the exercise up to now is that different communities start to speak to cyber communities; this makes the involved crisis management structures more aware of cyber risks". The spin-off exercise presented in Box 1, in particular, represents a good example of how the exercise has **raised awareness of NIS** among people who have limited knowledge of the area of cyber security and the work that ENISA is carrying out. Efforts at both of these levels will, over time, help to promote a culture of NIS in society.

However, **there is still a long way to go before a crisis management process is created at EU level in the cyber security area**, with a lack of trust among stakeholders, differences in national capabilities, weak communication structures, insufficient exchanges of information in "real life" etc., representing hurdles that need to be surmounted over the medium to long term.

Finally, it is important to note that interviewees concurred that ENISA had an important role to play within the area of cyber security, notably as "a trusted broker", an advisory body and in terms of the organisation of EU-level cyber exercises. ENISA "should continue what it is doing" as "what they do is good"; ENISA brings together the opinions and experiences of EU countries / cyber crisis agencies to raise awareness, educate, share lessons learned, and it also supports the streamlining of cyber security procedures throughout the EU. It was suggested that its role could be increased to act as a coordinator, creating technical capacities and providing 24/7 technical support on the basis of cyber security information being shared with it by Member States as "the current structures lack the type of leader that ENISA could be", the EU CERT playing this role for the EU institutions alone.

APPENDIX 1
INTERVIEW GUIDE

Interviewee type (i.e. Moderator, players, planners, EU CERT)	
Interviewee name	
Interviewee organisation / role	
Interviewer name	
Date	
Location	

Introduction

The interviewer will provide a brief overview of the focus (COAs, 2014), purpose, structure and timing of the evaluation overall. She will present the aim of the case study itself, i.e. to take a more in-depth look at one of ENISA's core operational activities in 2014 – the Cyber Exercise 2014.

The interview itself aims to ascertain whether the exercise is relevant, has led to changes in procedures and processes relating to emergencies and/or crises, and to what extent this has contributed to increased security, and seek interviewees' overall opinion on the exercise and suggestions for improvement. The aim of the interview is not to assess how well the exercise was organised.

Introductory questions

1. Please briefly explain your role, responsibilities and the length of time you have been in this role.
2. In what capacity and to what extent were you involved in the Cyber exercise 2014?

Contextual questions

3. Who are the key players / decision makers in the area of Cyber security that you would say form part of ENISA's target audience at national or EU level?
4. Do you have processes / mechanisms in place to respond to a Cyber security threat? To what extent have these been developed / undergone changes in recent years?
5. To what extent has ENISA played a role in helping to set up new / test existing/new processes mechanisms, e.g. through the 2014 Cyber Exercise?
6. To what extent was the Cyber 2014 exercise relevant and useful? Is it necessary to carry out such exercises? Why are you of this opinion?

Exchange of ideas, good practices and common exploration areas

7. Does the Cyber Exercise contribute to the sharing of information, ideas and common areas of interest during the actual exercise? If so, can you please provide an example?

8. Does this sharing of information, ideas and common areas of interest continue after an exercise has ended? Can you please give an example?

9. Are there any ways in which the exercise can be improved in order to encourage greater sharing of information, ideas and common areas of interest?

10. To what extent does the Cyber Exercise complement other public or private interventions? How would this be done without the support from ENISA?

Sharing of lessons learnt from exercises

11. Did you share the lessons learned from the exercises with other communities and sectors after the exercise took place? If so, with whom? How is this done?

12. To what extent should such lessons be shared more widely than they currently are? What means could be employed to do so?

Cooperation between operational communities

13. Do you now cooperate (more) with other operational communities with regard to emergency and/or threats than you did prior to the exercise? Is this increased cooperation a result of the exercise? Please provide examples.

14. If not, why not?

Improvement of services, workflows and communication to respond to emergency cases

15. Have the exercises improved work processes (speed of processing) and communication (information sharing) to respond to crises (joint responses to an emergency case)? If so, can you please give examples?

16. If not, what would it take to put in place effective and efficient emergency response procedures?

17. How could the exercises be improved in order to lead to further changes in this regard?

18. Have the exercises contributed to identifying gaps in the technical capacity of involved stakeholders to respond to a crisis situation? If so, please explain how. If not, why not?

19. Have the gaps identified been addressed? If so, how? If not, why not?

Development of mitigation and response strategies

20. Have the exercises supported the development of mitigation and response strategies? Can you please give examples?

21. Does ENISA contribute to putting in place cost effective procedures and mitigation and response strategies? What would have been the alternative, and would this have proved more or less costly?

22. Have you ever applied to real incidents the experiences gained in mitigation and response through the exercises? If so, how did it work? Can you please describe? Were the resource and time costs involved in line with your expectations?

Community building in Europe and beyond

23. To what extent do the exercises contribute to community building in Europe and beyond (between NIS specialists, entities?)? What would be an alternative to the exercises?

Concluding questions

24. A number of recommendations were made further to the 2014 Cyber exercise that need to be followed up on in the short, medium and long-term. To what extent have the short-term action points (deadline by end 2015) been followed up on? Please provide concrete examples.

Prompts:

	Actions on European Cooperation (as per AAR 2015)
A9	Establish a formal editorial team for the development of the EU-SOPs. Action owner: ENISA and Member States Timeframe: short-term
A10	Develop written procedures for the development of the EU-SOPs. Action owner: ENISA and Member States Timeframe: short-term
A11	Establish an update plan for the EU-SOPs. Action owner: ENISA and Member States Timeframe: short-term
A16	Adopt a consensual yet flexible approval process for the EU-SOPs. Action owner: ENISA and Member States Timeframe: short-term
A18	Establish a drafting and quality assurance process for EU consolidated analysis reports. Action owner: ENISA and Member States Timeframe: short-term
A20	Gather the requirements from MS for a cooperation platform. Action owner: ENISA Timeframe: short-term

25. What role does and should ENISA play within the area of cyber security? Why are you of this opinion?

26. Do you have anything else that you would like to add in relation to what we have discussed?