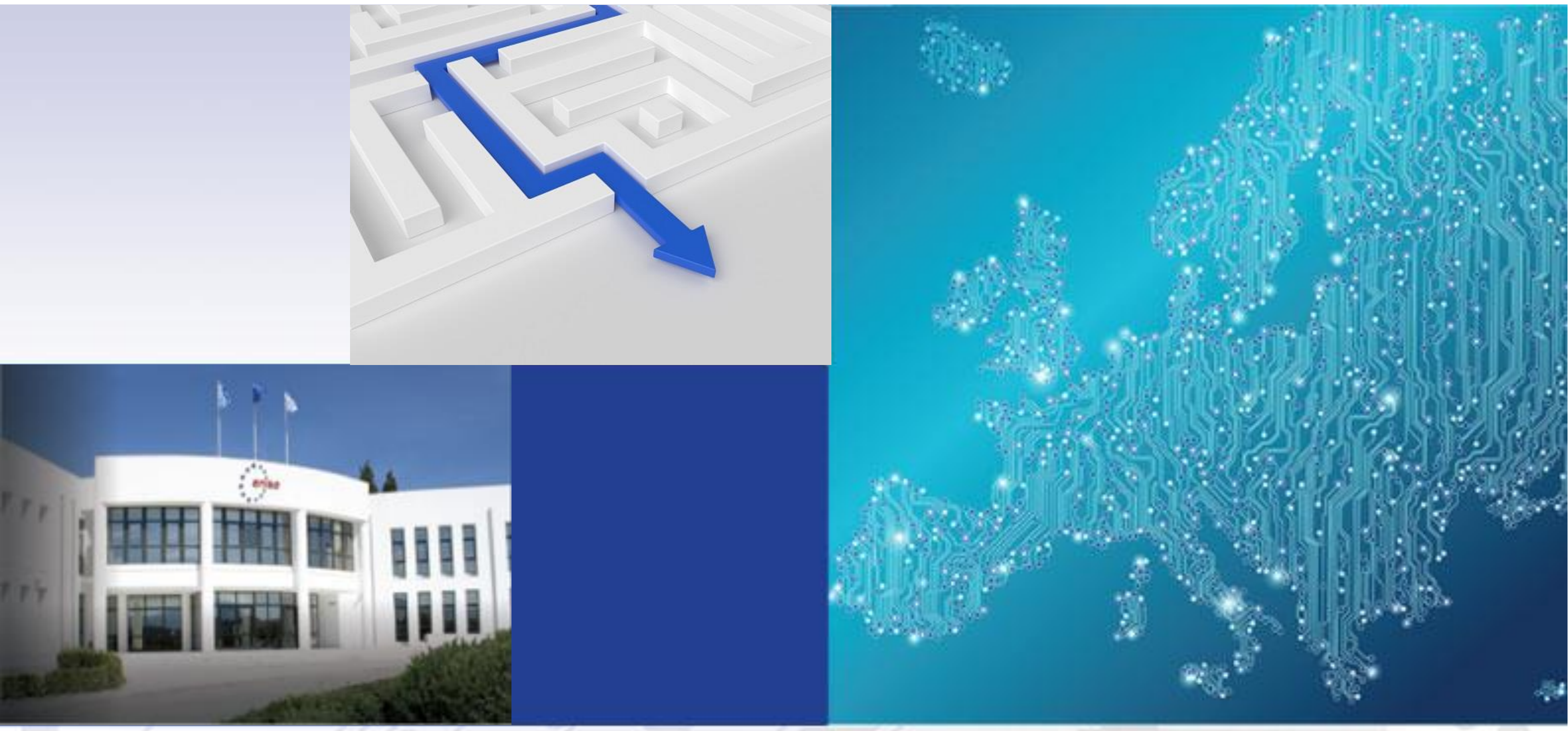


Leading the way

ENISA’s CSIRT-related capacity building activities

Impact Analysis – Update 2015

FINAL

VERSION 1.0

PUBLIC

NOVEMBER 2015

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Deloitte Reviseurs d'Entreprises / Bedrijfsrevisoren[1] Belgium

Lionel Ferette (ENISA)

Contact

For contacting, the authors please use cert-relations@enisa.europa.eu.

For media enquiries about this paper please use press@enisa.europa.eu.

Acknowledgements

As this document is essentially a review of the ENISA's work, it has been written by authors outside the ENISA. Nevertheless, the authors gratefully acknowledge the continuous support and appreciated feedback from Lionel Ferette (ENISA), Andrea Dufkova (ENISA), Panagiotis Trimitzos (ENISA), and their teams.

The authors would also like to thank the experts who took the time to be interviewed and/or fill out the online surveys, and whose opinions and views have informed many of the findings and suggestions of this study. A special thanks goes to the members of the ENISA "Operational Security" Unit and for their valuable contributions and insights during the internal workshop.

[1] Dan Cimpean, Anna Lauridsen, Alexander Cespedes Arkush, Dessislava Vitcheva, Patrick Kozakiewicz

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-132-8
DOI 10.2824/236326

Table of Contents

Executive Summary

Europe, like the rest of the world, is witnessing an unprecedented expansion in the cyber-security domain and an ever-growing community of CSIRTs (Computer Security Incident Response Team). In parallel, an evolving cyber threat landscape shows a sharp increase and levels of sophistication of cyber incidents and attacks. Against this backdrop, the relevance of ENISA (European Union Agency for Network and Information Security) and its role in networking and trust building, as well as capacity building to achieve high and effective levels of network and information security in the European CSIRT community, stands out. Undoubtedly, ENISA's support to achieve high and effective levels of network and information security within the European CSIRT community will remain an important cornerstone in the years to come. ENISA is uniquely positioned to spot the gaps and the needs of the community, and to lead the way towards sustained levels of cyber-security.

This report represents the update of an impact assessment performed by Deloitte of ENISA's capacity building activities for CSIRTs in 2014. This updated assessment serves as a basis for a proposed roadmap to 2020.

The impact of the ENISA support to the CSIRT community was assessed from a dual perspective - legislative and regulatory, as well as operational, with the key objectives to:

- Update the policy analysis;
- Gather additional input from practitioners, including specific input on the new duties;
- Together with ENISA, propose concrete projects or actions towards the roadmap implementation.

The legislative and regulatory perspective covers the objectives formulated in the ENISA regulation, the 2014 and 2015 ENISA Work Programmes, the Digital Agenda for Europe, the EU Cybersecurity Strategy and the proposed NIS Directive, as well as the EU Policy of Critical Information Infrastructure Protection (CIIP).

The operational perspective includes an assessment of the impact of ENISA's CSIRT support looking at four activity pillars:

- Baseline Capabilities for CSIRTs;
- Capacity building in sharing good practice and CSIRTs training;
- Supporting the CSIRTs in better collaboration with law enforcement agencies (LEAs);
- Cyber crisis cooperation and exercises.

The study was conducted using a multi-dimensional approach including document reviews, online surveys, one-to-one interviews and an internal ENISA workshop with input from key CSIRT experts.

The intended target audience for this study is for all interested in ENISA, yet primarily policy-makers, managerial staff, and senior experts in CSIRTs and other competent authorities in the EU Member States as well as senior EU level officials involved in activities supporting the work of CSIRTs across Europe.

The main results from the report have been included in a roadmap to 2020, including suggestions on concrete actions for ENISA's future CSIRT support.

The key findings can be summarised in the following points:

- **Legislative and regulatory perspective:** Based on the EU policies and strategy documents reviewed, it is evident that ENISA's role and impact in this domain is recognised and clearly reflected through the ever-increasing scope and authority extended over time to the Agency. For instance, the NIS Directive (final adoption pending) is expected to bring about important changes to the ENISA mandate.
- **Operational perspective:** Overall, the respondent views and findings concur with the findings of the 2014 report. ENISA is still considered to be the representative voice of the European CSIRT community and of other operational communities. Being uniquely positioned in the cybersecurity landscape, the CSIRT community welcomes the Agency to make use of its experience and to push the envelope by being bolder and taking a clearer stance in its publications, and proactively reaching out and endorsing initiatives when identifying them.
- As highlighted in the 2014 report, there is a need for ENISA to accommodate a 'two-speed' structure of CSIRTs, support less and more mature teams respectively. This is the case for the material the Agency produces, as well as for the trainings it organises. While the material pertaining to the baseline capabilities (activity pillar I) and capacity building (activity pillar II) remains vital contributions to the community, there is also a scope for the sharper technical focus of the ENISA reports, on the one hand and more policy oriented reports on the other.
- The awareness of ENISA's CSIRT support actions is high within the CSIRT community and overall there was a positive view of ENISA's CSIRT related work. There is still a strong support of ENISA's role as the facilitator and coordinator of the CSIRT community, serving as a middle ground mediator between the CSIRTs and the European Commission. ENISA bridges the gap between the technical focus of the CSIRTs and the political focus of the Commission. ENISA should also strengthen the ties between the CSIRTs and LEAs through further collaborating with the European Cybercrime Centre at Europol, Eurojust and CEPOL.
- The Cyber Europe exercises are appreciated by the CSIRT community. Suggestions for improvements include more advanced technical challenges to the exercises, and to manage the growing size of participants by grouping them regionally, while also inviting participations from the private. An increase in exercises focusing on more on crisis management is also welcomed.
- **360° Feedback:** Echoing the words of Commissioner Oettinger, ENISA was requested to explore a stronger mandate that would allow the Agency to drive the EU's technological independence. ENISA could play an instrumental role in the EU's ambition to regain 'digital sovereignty" and to reassert its digital independence. This new branch of strategic activities would examine the 'bigger picture', including industrial politics, and provide input in the form of strategic studies and workshops.

  Several respondents even pointed to the possibility for ENISA to expand its constituency (working increasingly with CSIRTs in various sectors) and coverage beyond the borders of the EU. For instance, there was a call for ENISA to enhance communication with non-EU countries and to establish minimal security standards for Member States on strategic and operational levels.

1 Introduction

ENISA strives to continuously improve the quality of its deliverables and their relevance for its stakeholders. The Agency has thus partnered with Deloitte to perform an impact Assessment of its work in the CSIRT area, and propose a roadmap for its future activities.

CSIRTs and operational communities are an essential target for capacity building, because they are in the field and address actual incidents. ENISA's activities that focus on this target group can have real world impact, through guidance with good practices as well as exercises that develop Member States develop crisis management capabilities. This report represents the outcome of a desk review, stakeholder survey, in-depth interviews, as well as an internal workshop conducted in Athens in April 2015 as a part of the evidence gathering for the project "Update of Impact Assessment and Roadmap".

1.1 State of Play – 2014 Impact Assessment

The background of the project is the 2014 "Impact Assessment & Roadmap" [1] performed by Deloitte with ENISA's support to Computer Security Incident Response Team for the period 2005 to 2014. The impact assessment has served as a basis for a proposed roadmap to 2020.

The key objectives of the study were to:

- Identify ENISA achievements in relation to European CSIRTs in light of relevant policy documents;
- Analyse the impact of these achievements and other operational communities;
- Provide a roadmap for the period leading up to 2020 based on the results of the impact analysis.

The study team assessed the impact of the ENISA support to the CSIRT community from a **legislative and regulatory perspective** on the one hand, and an **operational perspective** on the other.

The legislative and regulatory perspectives cover the objectives formulated in the ENISA Regulation [2], the 2013 [3] and 2014 [4] ENISA Work Programmes, and specific elements of other relevant acts, such as the Digital Agenda for Europe [5], the Cybersecurity Strategy of the European Union [6] and the proposed NIS Directive [7].

The operational perspective included an assessment looking at three activity pillars:

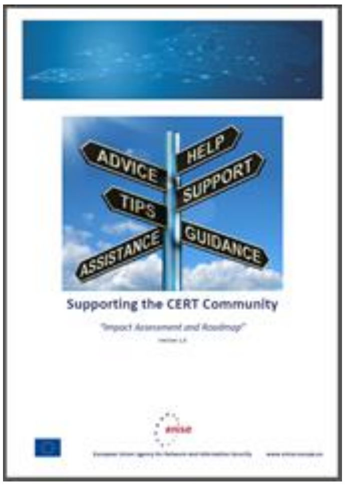
- Baseline Capabilities for CSIRTs;
- Capacity building in sharing good practice and CSIRT training;
- Supporting the CSIRTs in better collaboration with law enforcement agencies.

With the ongoing "Update of Impact Assessment and Roadmap" project ENISA aims to carry out a follow-up on the 2014 "Impact Assessment and Roadmap" on its impact in the area of support for CSIRTs.

The 2014 roadmap, which was validated by a group of CSIRT experts, is summarised below:

Legislative and regulatory perspective: Based on the EU policies and strategy documents reviewed, it is evident that ENISA's role and impact in this domain is recognised and clearly reflected through the ever-increasing scope and authority extended over time to the Agency. In the coming years, ENISA may act as a representative voice for CSIRTs in the European policy context.

Operational perspective: The awareness of ENISA's CSIRT support actions is high among the CSIRT stakeholders and overall there was a positive view of ENISA's CSIRT related work. However, awareness was higher among representatives of national and governmental CSIRTs than among other CSIRT communities (i.e. in the private, financial sector, etc.). As for the ENISA trainings, there was an expressed need to keep the baseline capabilities more separate from the capacity building activities as the former should cater to the needs of CSIRT teams of varied levels of maturity. Suggestions for future actions include a clear separation between supports to "new teams" vs. "advanced teams". This is linked to the request for greater clarity of the required level of prior knowledge needed to participate in different trainings. Regarding ENISA reports, there is a need for more technical topics on the one hand for the practitioners, and more policy-related reports on the other hand, serving to make the case of the ENISA *raison d'être* to policy and decision-makers. It was also suggested that ENISA should pick up topics and current trends/threats from the EU Member States and research them in-depth, as well as having them translated into several languages.


ADVICE
HELP
SUPPORT
TIPS
ASSISTANCE
GUIDANCE
Supporting the CERT Community
"Impact Assessment and Roadmap"
enisa

360° Feedback: Key points raised stressed that ENISA is the main CSIRT community connector and facilitator, within and beyond the traditional CSIRT stakeholder groups. ENISA's credibility as the voice of European CSIRTs within the EU and internationally was undisputed. Improved channels of information was another key point, requesting ENISA to better disseminate information via its website, related to both its activities, but also to alert the CSIRT community and other operational communities on current attacks and incidents. ENISA is also called upon to lead the work on compiling information on incidents and threats in a catalogue along with recommendations on how to handle them. The 360° feedback also included a call for greater harmonisation and common standards among CSIRTs under the lead and guidance of ENISA.

1.2 Study Purpose and Objectives

Although the 2014 report contributed with a wide array of stakeholder views on the ENISA CSIRT support, it was slightly impacted by a limited response rate to the survey and the project did not allow for much internal discussion on how to implement it. As a result, the proposals in the roadmap were primarily high-level recommendations. In addition, since the publication of the 2014 report, the responsibilities and resources of the ENISA "Operational Security" Unit have expanded to include cyber crisis cooperation and exercises. These were out of scope in the first study.

Therefore, the objectives of the "Update of Impact Assessment and Roadmap" are to:

- Update the analysis of relevant policy documents from regulation and from operational perspective;
- Gather additional input from practitioners, including specific input on the new duties;
- Together with ENISA, propose concrete projects or actions towards the roadmap implementation.

The main difference from the 2014 report is that the operational perspective of the update project includes a fourth pillar:

- Baseline capabilities for CSIRTs;
- Capacity building sharing good practice and CSIRT training;
- Support CSIRTs to better collaborate with law enforcement agencies;
- Cyber crisis cooperation and exercises.

In terms of the legislative and regulatory perspective it focuses on the objectives formulated in the ENISA Regulation, the 2015 Work Programme, the Cybersecurity Strategy of the European Union (and roadmap) and the proposed NIS Directive.

1.3 Policy Perspective

This chapter presents an overview of the results of the desk review, which was undertaken focusing on key strategic documents outlining the EUs policies influencing the domain, as well as the main official documents laying down ENISA's mandate and tasks related to support to CSIRTs. Additionally, views of respondents of both the interviews and surveys with regard to the policy and regulation perspective of ENISA's support activities have been incorporated where applicable. The information gathered has been grouped according to the following structure:

- ENISA Regulation;
- EU Policy of Critical Information Infrastructure Protection (CIIP);
- Cybersecurity Strategy of the European Union;
- Proposed NIS Directive;
- ENISA Annual Work Programme 2014 & 2015.

1.4 Operational Perspective

For the purpose of this document, the operational perspective of this study focuses on the following four pillars for capacity building:

- Baseline capabilities for CSIRTs;
- Capacity building sharing good practice and CSIRT training;
- Support CSIRTs to better collaborate with Law Enforcement;
- Cyber crisis cooperation and exercises.

The four pillars are treated in separate chapters in which we present the key points and suggestions that came out of the internal ENISA workshop, along with some of the feedback gathered from the respondents (surveys and interviews), on their views on these possible future activities of ENISA in the area of support to CSIRTs. We conclude each chapter with a draft roadmap to 2020 per pillar for the reader to have an overview of the suggested activities.

1.5 Target Audience

This study seeks to inform ENISA's stakeholders in a decision maker's role regarding its support activities until 2020 for CSIRTs and other operational activities. In addition, this study is intended to inform wider policy debates about how to make ENISA an even more valuable partner for national and governmental

CSIRTs and other relevant stakeholders in Europe and beyond, as well as to inform those CSIRTs and stakeholders about ways in which ENISA could support their work in the future. The study is also targeted at policy-makers, managerial staff, and senior experts in national and governmental CSIRTs and other competent authorities in the European Union Member States as well as senior EU level officials involved in activities supporting the work of CSIRTs across Europe.

1.6 Structure of this Report

The study consists of the following chapters. The introduction is followed by chapter 2, which outlines the study's qualitative methodological approach that combines a review of documents with online surveys and interviews with key experts in the field. Chapter 3 puts into context the policy perspectives which were taken into consideration for this study. This includes the European Union Policy on Critical Information Infrastructure Protection (CIIP), the Cybersecurity Strategy of the European Union, the proposed NIS Directive and ENISA's Annual Work Programmes for 2014 and 2015, while also presenting the responses of various stakeholders to the former. Chapter 4 illustrates the overall respondent views on the ENISA CSIRT support. These views have been grouped into three overarching themes focusing on their awareness, appreciation and perceived weakness of the related activites. The following four chapters, 5 to 8, concern themsleves with the operational perspective of this study reflecting the responsibilities and resources of ENISA related to its four operational pillars. These four chapters follow a similar structure, which starts off by describing ENISA's perspective on the road ahead, followed by the respondents views and concluding with a high-level roadmap to 2020. The final chapter 9, discusses the findings of the study and proposes a complete roadmap to 2020 for the four pillars.

2 Methodology

This study is supported by a desk review of the key legal and policy documents, interviews with key experts and online surveys with stakeholders from the CSIRT community and other operational communities. In the following chapters we present how the information collection for this study was undertaken.

2.1 Definitions

The purpose of this chapter is to provide the reader with an overview of what is understood, within the framework of this study, by "deliverables", "activities" and "CSIRT community support":

THEME	DESCRITPTION
Deliverables	• Reports and studies • Training guides and exercises • Awareness materials
Activities	• Trainings • Support to the set-up of CSIRTs • Workshops • Technical part of Cyber Crisis Cooperation exercises
CSIRT community support	• Participation in conferences and events (incl. as speaker) • Meeting facilitations (between CSIRTs and other actors) • Liaising, co-operation and information exchange initiatives • Provide advice

In order to further facilitate for the reader of what is understood by "deliverables", "activities" and "community support" in the remainder of this report we have added a number of concrete examples. This list of examples is non-exhaustive, but it does display a wide variety of ENISA CSIRT related actions.

"**Deliverables**" are all materials (reports, studies, training guides and exercises and awareness materials, etc.) that ENISA makes available to the CSIRT community, either though closed distribution channels or through their website, such as:

- The studies on Building a CERT and Running a CERT [8];
- Good practice guide for incident management [9].
- Good Practice Collection for CERTs on the Directive on attacks against information systems [10].

"**Activities**" includes open and closed meetings (by invitation only), trainings, set-up of CSIRTs, exercises and workshops, etc., such as:

- Annual national and governmental CERT workshops [11];
- ENISA Train the trainers and multipliers workshop [12];
- ENISA-EUROPOL/EC3 workshops [11];
- TRANSITS training support [13];
- Technical part of Cyber Europe Exercises [14].

"**Community support**" englobes ENISA activities and deliverables that are of a more *ad hoc* nature and therefore less visible on the ENISA website and through other communication channels, such as:

- Meeting facilitations (between CSIRTs and other actors);
- Liaising / raising awareness;
- European CSIRT Community – TF-CSIRT [15] and FIRST [16].

2.1.1 Time line for the proposed roadmap

In the proposed roadmap following this report, we refer to actions and activities to be implemented in the short, medium and long term, by which we suggest the following:

- Short term: within the next year (2016/17)
- Medium term: 2-3 years (2018/19)
- Long term: 4 years and beyond (2020 and after).

2.2 Information Collection

2.2.1 Desk study

A number of key documents have served as a foundation for the study to identify the legal and policy framework of ENISA's CSIRT-related mandate, activities and performance with regards to supporting the CSIRTs and other operational communities. The overview below provides a list of the key documents that have been reviewed within the scope of the desk study of this report:

- EU Policy of Critical Information Infrastructure Protection (CIIP);
- Cybersecurity Strategy of the European Union;
- Proposed NIS Directive;
- ENISA Annual Work Programme 2014 & 2015.

2.2.2 ENISA internal workshop

An ENISA internal workshop has been conducted in Athens in April 2015 as a part of the evidence gathering for the project, by including the key ENISA experts that are involved in the CSIRT-related activities of the Agency. Upon the completion of the workshop and validation by ENISA staff, the main points coming out of this workshop were summarised and included in this report.

2.2.3 Online survey

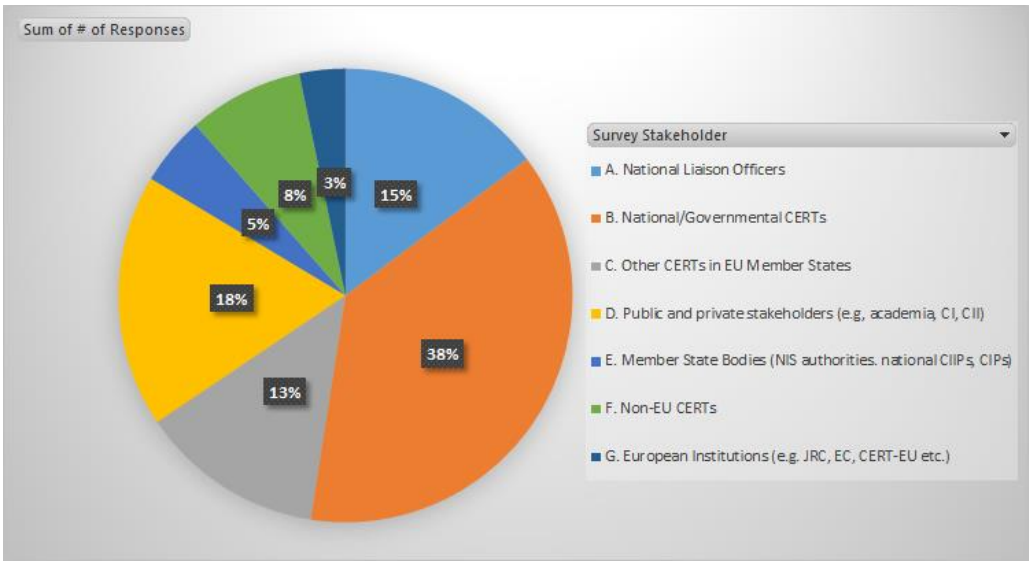
One of the key instruments used for data collection for this study was an online survey, which was hosted on the European Commission's 'EUSurvey' platform. The study team has designed the online survey questionnaire in order to provide:

- A clear structure with a straightforward presentation of questions and possible answers;
- An easy monitoring of the survey progress and results.

Selected experts from seven stakeholder groups were contacted and invited to participate in the online survey. The table below presents the share of respondents (as percentage) per stakeholder group.

STAKEHOLDER GROUP	(%)
National Liaison Officers	15%
National CSIRTs & Governmental CSIRTs	38%
Other CSIRTs in EU Member States.	13%
Non-EU CSIRTs	8%
European Institutions (e.g. JRC, EC, CERT-EU etc.)	3%
Member State Bodies (NIS authorities. national CIIPs, CIPs)	5%
Public and private stakeholders (e.g. academia, CI, CII)	18%

Figure 1 – share (%) of respondents by group



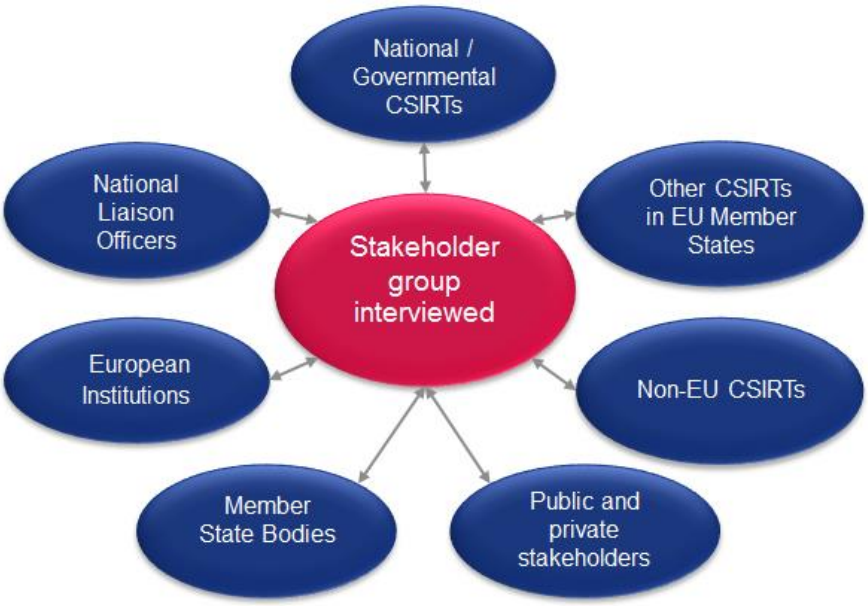
2.2.4 Interviews

The list of respondents interviewed was selected by ENISA. The study team conducted the interviews, either in person (with the stakeholders located in Brussels, Belgium) or via phone. The interviews were conducted between June and September 2015.

The interviews were pursued in a semi-structured manner allowing for auxiliary questions and for new lines of questioning depending on the responses of the respondents. During the interviews, the study team followed an agreed-upon protocol covering all the different themes that were treated during the interview with the selected CSIRT stakeholders. However, interview respondents were free to discuss additional relevant topics they considered as important or interesting.

Only note taking was used to capture the content of the interviews. Referencing to Chatham House rules, interviewees were assured of non-attribution and anonymity when using direct quotes, unless they gave the study team explicit permission to be quoted. As a result, in reporting on the interviews in this study, a quasi-anonymous approach is pursued, with references only being made to participant's role or type of host organisation, i.e. CSIRT, LEA, policy-making body, or other.

Figure 2 – Overview of host organisations of interview respondents


National / Governmental CSIRTs
National Liaison Officers
Other CSIRTs in EU Member States
Stakeholder group interviewed
European Institutions
Non-EU CSIRTs
Member State Bodies
Public and private stakeholders

2.3 Stakeholder Categories

2.3.1 National Liaison Officers

ENISA has set up a network of National Liaison Officers (NLOs), which serve as ENISA's contact point with the Member States on specific issues. ENISA also gains access to a network of national contacts through individual NLOs, reinforcing the activity of the Agency in the Member States.

Member States representatives – one from each EU and EEA country – are part of the NLO network. A representative from the European Commission and a representative from the Council of the European Union are also part of this network.

2.3.2 National/Governmental CSIRTs

National and governmental CSIRTs are Computer Security Incident Response Teams (CSIRTs) that serve the government of a country by helping to protect the critical information infrastructure. National and governmental CSIRTs play a key role in coordinating incident management with the relevant stakeholders at the national level. They also bear the responsibility for cooperation with the national and governmental teams in other countries.

2.3.3 Other CSIRTs in EU Member States

This stakeholder group represents CSIRTs which are located in the European Union but not mandated by the government. Examples include among others CSIRTs in research and education, as well as military CSIRTs.

2.3.4 Non-EU CSIRTs

This stakeholder group represents CSIRTs which are located outside of the European Union. Examples include CERT-GIB, Swisscom and SWITCH-CERT.

2.3.5 European Institutions (e.g. JRC, EC, CERT-EU etc.)

The institutions of the European Union include the European Commission, the European Parliament, European Agencies such as JRC, and CERT-EU.

2.3.6 Member State bodies (NIS authorities. national CIIPs, CIPs)

This stakeholder group includes professionals from the national authorities dealing with information security and issues related to CSIRT activities. Examples include, NIS and cyber-security bodies.

2.3.7 Public and private stakeholders (e.g. academia, CI, CII)

This group includes any other public or private organisation that relates to CSIRT activities. Examples include professional services, associations of providers and legal & policy experts.

3 Policy Perspective

This chapter presents an overview of the results of the desk review, which was undertaken focusing on key strategic documents outlining the EUs policies influencing the domain, as well as the main official documents laying down ENISA's mandate and tasks related to support to CSIRTs. Additionally, views of respondents of both the interviews and surveys with regard to the policy and regulation perspective of ENISA's support activities have been incorporated where applicable. The information gathered has been grouped according to the following structure:

- EU Policy of Critical Information Infrastructure Protection (CIIP);
- Cybersecurity Strategy of the European Union;
- Proposed NIS Directive;
- ENISA Annual Work Programme 2014 & 2015.

3.1 EU Policy of Critical Information Infrastructure Protection (CIIP)

The European Commission Communication [17] on Critical Information Infrastructure protection focusing on the protection of Europe from cyber disruptions by enhancing security and resilience was adopted in 2009. The Communication included an action plan based on five pillars, involving the Member States and the private sector:

- Preparedness and prevention;
- Detection and response;
- Mitigation and recovery;
- International cooperation;
- Criteria for European Critical Infrastructures in the field of ICT.

The CIIP Ministerial Conference organised by the Hungarian Presidency of the EU in 2011 served as a forum to evaluate progress, assess lessons learnt and to discuss the remaining challenges ahead and next steps. The following 2012 European Parliament Resolution on "Critical Information Infrastructure Protection: towards global cyber security" [18] made further recommendations to the Commission. Several of these were echoed in the Cybersecurity strategy and in the proposal for a Directive on network on information security (hereafter "the NIS Directive") published in 2013.

Among the key achievements related to the CIIP policy, brought about by ENISA include:

- The adoption of a minimum set of baseline capabilities and services, and related policy recommendations for national/governmental Computer Emergency Response Teams to function effectively;
- The carrying out of pan-European exercises, (i.e. Cyber Europe 2010, 2012, etc.)

Whilst the EU Cybersecurity Strategy did include certain actions, such as the pan-European exercises, the voluntary nature of the CIIP policy [19] has been seen as a weakness, which could be amended by the adoption of the NIS Directive. This would require the Member States to put in place a minimum level of capabilities at national level and to cooperate across borders [20].

3.2 Cybersecurity Strategy of the European Union

The Cybersecurity Strategy of the European Union [6] outlines the EU's vision in the domain of cyber security, clarifying roles and responsibilities, and specifying required actions to promote online security and citizens' rights.

The vision presented in the Strategy is articulated in five priorities and foresees a key role for ENISA in protecting Europe's cyberspace in the first and the fourth priority to 'achieving cyber resilience' and to 'develop industrial and technological resources for cybersecurity'.

> "ENISA's role in supporting the Cybersecurity Strategy is really important and ENISA does it very well."
> Respondent from a Member State body

To boost cyber resilience in the EU, both the public and the private sector must develop capabilities and cooperate effectively. In the second priority of the Strategy the Commission asks ENISA to:

- Assist Member States in developing strong national cyber resilience capabilities, by building expertise on security and resilience of industrial control systems, transport and energy infrastructure;
- Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU [21];
- Continue supporting the MS and the EU institutions in carrying out regular pan-European cyber incident exercises which will also constitute the operational basis for the EU participation in international cyber incident exercises.

To develop industrial and technological resources for cybersecurity, in the fourth priority of the Strategy the Commission asks ENISA to:

- Propose in 2013 a roadmap for a 'Network and Information Security driving licence' as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators);
- Develop, in cooperation with relevant national competent authorities, relevant stakeholders, and international and European standardisation bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.

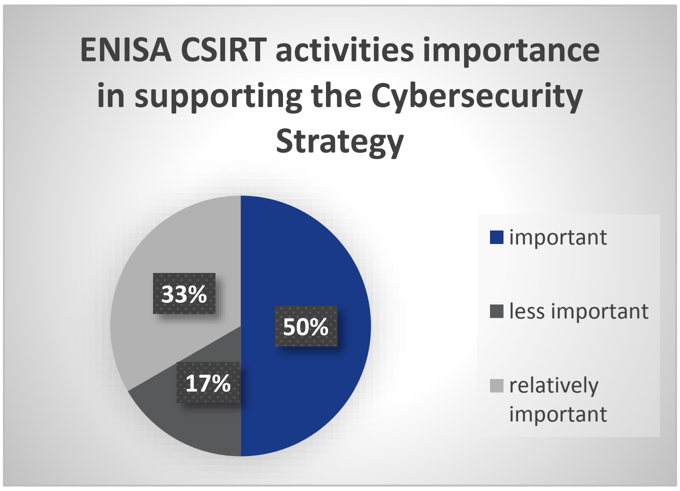
The Cybersecurity Strategy of the European Union is not a legally binding document, however ENISA is expected to take into account these requests coming from such a high level document.

3.2.1 Respondent views

The respondents were asked what additional CSIRT-related areas and activities, in line with the Cybersecurity Strategy of the EU, they would recommend ENISA to focus on for the coming five years. Respondent from national CSIRTs suggested that ENISA should prioritise CSIRT capacity building, training and exercises. However, when it comes to incident handling, it is believed that ENISA should not handle incidents now or in the coming five years. Most of the respondents believe that ENISA should concentrate more on organising trainings and workshops with emphasis on technical aspects.

Other respondents stressed that while the European cyber exercises are extremely helpful, there is a need for a European cyber crisis system. This was deemed to be a difficult task for ENISA since the decisions on crisis management remain mainly at the national level and ENISA does not have a mandate outside the area of NIS.

In addition, the table below illustrates the results from the 'EUSurvey' platform, demonstrating that over 80% of the responding National Liaison Officers believe that ENISA CSIRT related activities are of importance in supporting the Cybersecurity Strategy of the European Union.



The respondents were asked to what extent they believe that ENISA capacity building activities are important in supporting the Cybersecurity Strategy of the European Union, in particular the goals related to co-ordination between NIS competent authorities, CSIRTs and law enforcement. Most of the respondents agreed that ENISA capacity building activities are important in supporting the Cybersecurity Strategy of the European Union and in particular the goals related to co-ordination between NIS competent authorities, CSIRTs, and law enforcement. However, one of the respondents did not completely agree with this statement and expressed that according to him, there is still a lot to be done in this direction and that cooperation between those three authorities is still not in good state due to cultural differences.

Furthermore, the respondents, with respect to the Cybersecurity Strategy of the European Union, suggested that ENISA should focus on the following:

- **Trust building**: Several respondents recommended that ENISA continues this and some proposed the following:
  - ENISA engages more with senior policy makers to outline that cyber security matters;
  - Secondment and staff exchanges between CSIRTs in other Member States, and between Member States and EU institutions. Enhancing communication with non-EU countries;
- **Cooperation**: ENISA should build on this basis by serving as a coordinator as it already has established good relations with CSIRTs and develop upon its existing cooperation network to expand to other sectors, industries and stakeholders. In addition, CSIRTs are very often not very well connected to private companies' CSIRTs and this could be promoted by supporting CSIRT associations like CERT-Verbund in Germany. Some respondents even mentioned, which would go beyond the remits of the ENISA mandate, enhanced cooperation with the military sector. In addition, ENISA could provide a secretariat and guidance function for the CSIRT network in view to harmonise differences between MSs;
- **Training:** Tailored trainings and exercises, for example for incident handlers, liaisons, analysts, press contacts, etc. ENISA can also conduct trust building measures and capacity building, coordinate

technical/operational trainings, enhance training material, support tool building initiatives, and support the CSIRT needs. This could include the Connecting Europe Facility (CEF)[2].

- **Materials:** Provide guidance materials and reports and act as a repository or a "go-to place" in terms of having a broad source of information whether the materials are produced by ENISA or others.

3.3 Proposed NIS Directive

The proposed NIS Directive [7] is a legislative instrument, pending final adoption by EU Council Ministers and the EU Parliament, to support the achievement of some of the high level goals identified in the Cybersecurity Strategy, including promoting a high common level of NIS by improving internet security, private networks, and information systems. The proposed NIS Directive lays down measures to ensure a high common level of Network and Information Security (NIS) across the EU:

- Establish common minimum requirements for NIS at national level;
- Set up coordinated prevention, detection mitigation and response mechanism, enabling information sharing and mutual assistance amongst the national NIS competent authorities;
- Improve preparedness and engagement of the private sector.

The proposed NIS Directive elaborates on the role of ENISA with regard to supporting Member States and the EU by assisting in the operation of the cooperation network, providing Member States and the EU with its expertise and advice, and by facilitating the exchange of best practices. The proposal also suggests that ENISA should cooperate with the EU institutions and Member States to develop a cooperation plan to counter risks and incidents.

3.3.1 Respondent views

In relation to the NIS Directive, one respondent from the NLOs stated that ENISA should focus on how it can help on the effective implementation of the NIS directive. In relation to article 8 of the NIS directive on the formation of a cooperation network, one respondent from a governmental CSIRT called for ENISA's already existing cooperation with CSIRTs to be fully used and for its role to be crystallised in order for ENISA to serve as a coordinator, so as to not duplicate efforts. In the current version of the proposed Directive, ENISA is only to assist the cooperation network when requested to. It was also stressed in the interviews that ENISA should develop operational procedures in support of new activities, if requested. Moreover, as the NIS Directive is a work in progress, ENISA should "not create additional work for itself by overstepping their current mandate".

Other responses highlighted the need for ENISA's role in assisting in the effective implementation of the NIS directive:

- NIS community support;
- NIS stakeholder brokerage and trust-building Initiatives between MS CSIRTs;
- Policy support for EU bodies and MS;
- Set up of an information hub for the NIS community;
- CSIRT functionality assessment for regulatory compliance with the NIS Directive;

[2] http://ec.europa.eu/digital-agenda/en/connecting-europe-facility

- CSIRT baseline capabilities assessment and regulatory self-assessment toolkit.

It is also important to consider that 80% of the European Institutions and Member State Bodies respondents have a neutral response to whether ENISA should develop operational procedures to support new activities introduced by the proposed NIS Directive. This could be due to the fact that the NIS Directive is still under negotiation by competent institutions.

3.4 ENISA Regulation

The new ENISA Regulation [2], constitutes the most recent ENISA mandate and replaces the prior Regulation from 2004. It guarantees the operations of ENISA until 2018 and provides the Agency's general strategy, building on ENISA's achievements in areas such as support to CSIRTs in Member States and facilitation of pan-European cybersecurity exercises.

The new Regulation enlarges the scope of ENISA and its authority to make an even bigger differ-ence in protecting Europe's cyberspace, including ENISA supporting the development of EU cyber-security policy and legislation. In terms of ENISA CSIRT support activities, the Regulation lays down a number of expectations in relation to national and governmental CSIRTs and other CSIRTs in Europe, which are summarised below.

- CSIRT Operational Frameworks and Mandates: Facilitation of the emergence and maintenance of a stable national and governmental CSIRT architecture across the EU, which also provides overarching framework for EU information security.
- CSIRT Service Portfolios: ENISA support to the formulation of a peer review system amongst national and governmental CSIRTs to assess performance against a common set of capabilities.
- CSIRT Resources: ENISA support for strengthened capabilities of national and governmental CSIRTs that should also establish a common set of operational capability criteria. These should also match those of the 'most developed CSIRTs' in the EU.
- Cooperation: The Regulation tasks ENISA to "promote cooperation and the exchange of information and best practices' between CSIRTs and other relevant organisations", and also gives ENISA a greater interfacing ability with the European Cybercrime Centre, providing for a more proactive ENISA role with regard to encouraging information exchange amongst national and governmental CSIRTs and LEAs.

3.5 ENISA Annual Work Programme 2014 & 2015

3.5.1 ENISA Work Programme 2014

The 2014 Work Programme [3] stressed that ENISA's strategic priorities are designed to support Member States' efforts to meet EU policy objectives. The Work Programme reflects the fact that ENISA obtained new tasks to perform during 2014 following its new mandate and the Cybersecurity Strategy for the European Union. In this context, ENISA identified three Work Streams that define its current core operational activities:

- WS1: Support EU policy building;
- WS2: Support capacity building;
- WS3: Support cooperation.

Since not all work streams included CSIRT related tasks for ENISA, the desk review focused on work packages 2.1 and 3.3 as described below.

3.5.1.1 Work Package 2.1: Support Member States' Capacity Building

Work Package 2.1 aimed at improving the operational activities of CSIRTs through the following:

- Stock-taking of achievements, good practices and experience with a view to develop a road map;
- Enhance training and exercise methodology to improve the competencies of trainers;
- Produce good practice guides on training methodologies for CSIRTs derived from experiences in delivering suitable CSIRT training;
- Provide an update of the "baseline capabilities" definition and to draw conclusions for new training materials. In addition, ENISA will deliver a new set of CSIRT exercise material with at least five new scenarios covering the four main baseline capabilities competencies, including operational, technical, mandate and cooperation competencies.

3.5.1.2 Work Package 3.3: Regular Cooperation among NIS Communities

Under the Work Package 3.3, ENISA implemented activities with the aim to:

- Actively support or organise common trainings for different communities, such as CSIRTs and LEAs;
- Engage with the European Cyber Crime Centre (EC3), where appropriate, through formal and informal cooperation channels;
- Take stock of the response of other communities to cyber security challenges and establish how they could inform the works of CSIRTs;
- Facilitate the outreach to other bodies and /or communities, including taking stock of accepted methods for trust building within and among communities;
- Continue to collect good practice useful for CSIRTs and LEAs and to enhance ENISA exercise and training materials.

This work package extended the scope of ENISA's support to the communities dealing with NIS to non-operational communities, to enable communications between CSIRTs, law enforcement, financial and other communities. Activities scheduled to implement these goals included ENISA to utilise the 9th ENISA CSIRT workshop to prepare future work in the area of CSIRT training and CSIRT cooperation with LEAs in collaboration with the European Cybercrime Centre (EC3). ENISA also engaged in the formulation of a good practice guide and/or training and exercise materials concerning the exchange and processing of actionable information by CSIRTs, as well as in the drafting of good practice materials for first responders in cooperation with the EC3. Moreover, as a part of this work package, ENISA prepared and published the reports "Stocktaking of standards formats used in exchange of processing actionable information" [22], and "Scalable and Accepted Methods for Trust Building in Operational Communities" [3].

3.5.2 ENISA Work Programme 2015

In 2015, the ENISA work streams were permanently replaced by strategic objectives, which in turn are aligned with the ENISA Strategy document and the multi-annual planning (2015-2017) [23].

The ENISA strategic objectives for 2015 are as follows:

- SO1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS);
- SO2: To assist the Member States and the Commission in enhancing capacity building throughout the EU;
- SO3: To assist the Member States and the Commission in developing and implementing the policies necessary to meeting the legal and regulatory requirements of Network and Information Security;
- SO4: To enhance cooperation both between the Member States and the EU and between related NIS communities.

> "There is disconnection between the operational and political levels, and ENISA is good at trying to fill this gap."
>
> Respondent from the European institutions

As was the case in previous years, CSIRT related tasks were not included in all strategic objectives, and therefore our desk review focused on work packages 1.4, 2.1, 4.1 and 4.2 as described below.

3.5.2.1 Work package 1.4: Short- and mid-term sharing of information regarding issues in NIS

The objective of this works package is to allow the Agency to provide timely and qualitative responses to NIS developments through the definition and implementation of a framework. As regards CSIRTs the aim is to improve the information flows between the CERT EU, ENISA and the CSIRT community at large.

3.5.2.2 Work package 2.1 Assist in public sector capacity building

This work package aims to assist CSIRTs, and other operational communities, as appropriate to develop and extend the necessary capabilities in order to meet challenges to secure their networks. By doing so, CSIRTs and other operational communities will benefit from trainings and tailor-made capability enhancement actions.

3.5.2.3 Work package 4.1 Support for EU cooperation initiatives amongst NIS-related communities in the context of the EU Cyber Security Strategy (EU CSS)

The aim of this work package is to continue to build up targeted NIS communities to meet policy goals. Specifically, the work package will exploit the good experiences of the Agency from its support to CSIRTs, the CSIRT communities and Law Enforcement communities in order to identify mutually satisfactory ways to collaborate. ENISA will develop and provide guidance leveraging best practice for cooperation between stakeholder communities, including CSIRTs, the CIIP community, law enforcement and financial services, etc. In the spirit of building communities through 'learning by doing', ENISA will continue its support of the TRANSITS training in the area of CSIRTs.

ENISA's support to the collaboration between CSIRT and law enforcement communities, including close collaboration with other institutions such as EC3 (Europol). In this vein, the agreement between ENISA and EC3 will be further developed to include a more operational and systematic flows of expertise, elaboration of general situational reports, reports resulting from strategic analyses and best practice, enhancing capacity building through training and awareness raising in order to safeguard network and information security at the EU level. To this end, ENISA will stay engaged in the EC3 programme board.

3.5.2.4 Work package 4.2 European cyber crisis cooperation through exercises

The aim of this work package is to facilitate the planning of the upcoming pan-European Cyber Exercise in 2015-2016. To this end, ENISA will further develop its methodology, training outreach and technical capability to organise large-scale cyber crisis exercises. In practice, this translates into three following topics:

- Pan-European cyber exercises management (Cyber Europe and EuropeSOPEx);
- Enhance capacity to support and organise cyber exercises;
- Promote, maintain and improve EU cyber crisis cooperation plans and procedures (i.e. EU SOPs), including bringing close the cyber crisis cooperation community [23].

3.5.3 Respondent views

When asked to what extent the respondents agreed with the statement that ENISA has successfully implemented the capacity building activities included in this study (i.e., CSIRT support and Cyber Crisis Cooperation and Exercises related activities) set out in the Annual Work Programmes, in the past five years, the respondents, in particular the National Liaison Officers indicated an overall agreement. This is further confirmed by the online survey with 73% of the National Liaison Officers and European Institutions respondents agreeing.

One EU official stated that while he did not have a detailed overview of the ENISA CSIRT support, he had noted that "ENISA has established good cooperation at various levels with CSIRTs and at a personal level", during past ENISA Cyber Exercises which he had attended. "They speak the same language", the official continued. In this respect, it seems that ENISA has established cooperation on all levels. However, the challenge is what happens at the top political level. In the event of a crisis, decisions need to be taken fast, which requires a solid understand of the sector.

The EU official also noted that in the cyber domain "jargon is a killer", which makes it harder for "non-techie" staff to understand the issues. However, ENISA is perceived to be doing a good job in bridging the gap between the operational and policy levels, given the Agency's size and the fact that the bar is continuously being raised.

3.6 Policy perspective - Summary table of ENISA impact

The following table summarises key ENISA capacity building activities of the European Union Policy of Critical Information Infrastructure Protection (CIIP), Cybersecurity Strategy of the European Union, Proposed NIS Directive and ENISA Annual Work Programme 2014 & 2015 and provides conclusions on how ENISA has responded to them.

POLICY	PROPOSED ENISA CSIRT RELATED ACTIVITIES	CONCLUSION
EU Policy of Critical Information Infrastructure Protection (CIIP)	The Commission has asked ENISA to: • Carry out pan-European exercises • Adopt a minimum set of baseline capabilities and services and related policy recommendations for (CSIRTs) to function effectively.	ENISA has carried out Cyber Europe Exercises in 2010, 2012 and 2014 and will continue to do so in 2016. ENISA has established various baseline capabilities and services to CSIRTs (capability materials, technical updates, improved communication, enhanced information sharing, etc.)

POLICY	PROPOSED ENISA CSIRT RELATED ACTIVITIES	CONCLUSION
Cybersecurity Strategy of the European Union	The Commission asks ENISA to: • Assist MS in developing cyber resilience capabilities; • Examine the feasibility of ICS-CSIRTs; • Continue support-EU cyber incident exercises;	ENISA has continued to encourage good practices in information and network security to ensure its assistance and support to Member States in developing strong national cyber resilience capabilities. ENISA has done so by supporting and organising pan-EU cyber incident exercises, trainings and workshops, and by building on expertise, cooperation and support on security and resilience of industrial control systems, transport and energy infrastructure, etc. Regarding the roadmap for a 'NIS driving licence,' ENISA has started the consultation process in order to involve the relevant stakeholders and guide the process in order to ensure quality results.
Proposed NIS Directive3	The Commission would ask ENISA to: • Assist in the operation of the cooperation network; • Provide MS and the EU with expertise and advice; • Facilitate the exchange of best practices.	The Network and Information Security Directive was proposed by the Commission in 2013 and is currently in the final stages of negotiations between the European Parliament and the Council.
ENISA Annual Work Programme 2014 & 2015	The 2014 & 15 WP outlined the following ENISA support to CSIRTs: • Support Member States' Capacity Building • Regular Cooperation among NIS Communities • Short- and mid-term sharing of information regarding issues in NIS • Assist in public sector capacity building • Support for EU cooperation initiatives amongst NIS-related communities in the context of the EU Cyber Security Strategy (EU CSS) • European cyber crisis cooperation through exercises	ENISA supported the communities dealing with NIS to non-operational communities, enabling communications between CSIRTs, LEAs, financial and other communities. Capacity building, trainings, workshops, exercises and dissemination of good practices. Facilitating cooperation and coordination between public and private stakeholders. ENISA implemented the operational security activities (i.e. CSIRT support and Cyber Crisis Cooperation and Exercises related activities) set out in the Annual Work Programmes. ENISA enhanced cooperation with LEAs and the EC3.

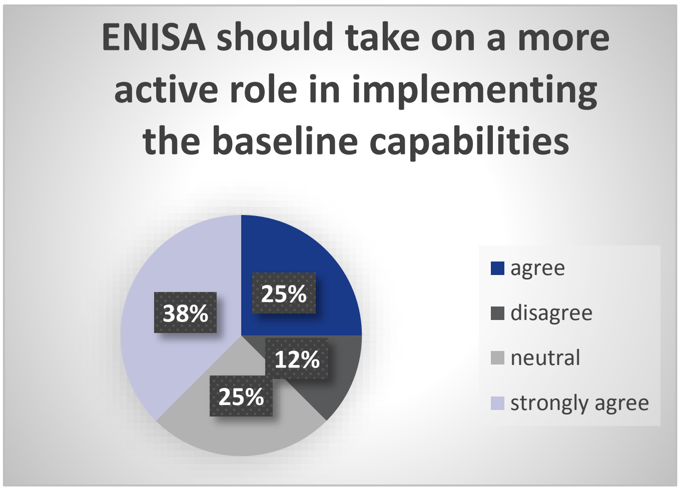
[3] At the time of writing, adoption of the NIS Directive is pending. However, no significant changes are expected to the proposed directive.

4 Overall Respondent views on ENISA CSIRT Support

The following chapter reflects the respondents' awareness, appreciation and perceived weakness of the ENISA CSIRT support. It is important to note that most of the views expressed by the respondents did not deviate far from the ones of last year's report covering the same parts.

4.1 Respondent awareness of related activities

A majority of the respondents are aware of ENISA's activities in carrying out baseline capabilities, capacity building, sharing of good practices and CSIRT trainings. When asked whether ENISA should take a more active role in implementing baseline capabilities, a majority of the respondents agreed with the suggestion. One respondent proposed that ENISA could further increase awareness about its tasks by taking a more 'marketing' approach to widening its reach, as its work is valuable, needed and more stakeholders should be aware of it.



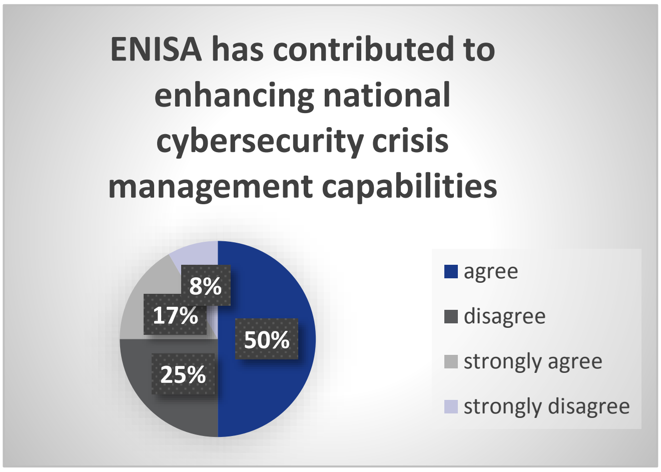
All of the respondents were aware of ENISA's website and mailing list and all had experience with ENISA CSIRT trainings or relevant material. Moreover, almost half of all the respondents had recently attended an ENISA CSIRT-related event (e.g. workshops, cyber exercises, trainings etc.). Some respondents, predominately from the European Institutions noticed the lack of ENISA trainings for European Officials and remarked that such trainings would be very beneficial for them.

4.2 Respondent appreciation of related activities

The majority of respondents appreciate ENISAs CSIRT support. This is reflected by the fact that a large majority of the National CSIRTs and Governmental CSIRTs, MS Bodies and Public and Private Stakeholder respondents agree that ENISA's CSIRT related support and activities evolve in line with the needs and priorities of the CSIRT community.

> "ENISA training materials are very useful and we use them often."
>
> Respondent for the Public/Private Sector

Moreover, most respondents stated that they are satisfied with ENISA's role as a networker for the community and believe that ENISA should continue working as a facilitator, coordinator and a trusted introducer, disseminating good practices and bringing CSIRTs and relevant stakeholders together. There is also an incentive for ENISA to further develop its methods and techniques for identifying gaps and help to achieve stronger cooperation. When asked about the usefulness of ENISA's CSIRT related events, respondents were in agreement that it they are useful.



Furthermore, as illustrated in the chart, a majority of respondents agree and appreciate ENISA contributing to enhancing and supporting national crisis management capabilities.

Finally, the respondents acknowledge and appreciate that sufficient means and channels are available to the CSIRT community in order to provide ENISA with feedback, suggestions and questions on its CSIRT related activities.

4.3 Perceived weakness of related activities

The perceived weaknesses focused on the issues of costs, cooperation and crisis management. Some Member State Bodies, National CSIRTs and Governmental CSIRTs stressed that the costs of traveling to ENISA workshops often times exceed the budgets. However, as mentioned by a different respondent, ENISA organises them in different places every year, with the help of a local host. In other words, travel expenses could be reduced if a CSIRT hosted the workshop. Likewise, respondents shared that they would like to see the topics and presentations at ENISA's CSIRT related events to be more focused on practical, technical and relevant areas for CSIRTs, such as exercising, and avoid wider policy topics.

In addition, according to respondents, the cooperation between the Operational Security Community and the EU Institutions and its Agencies is still insufficient and needs to be further improved. They believe that the reason for this relates to cultural differences among Member States. To illustrate, a respondent gave the example that what is qualified as a cybersecurity incident in one country could be qualified as terrorism in another.

Respondents also mentioned that CSIRTs focus on large-scale incidents and ENISA could support CSIRTs in handling small incidents, because 'not handling these small incidents, builds the ground for large scale attacks.' In addition, some respondents mentioned that ENISA could play a greater role in supporting CSIRT connections with industry and the private sector to ensure good practises are more widespread outside of the current National CSIRT environment. Respondents also mentioned that ENISA could support CSIRTs by enhancing communication with non-EU countries and by establishing minimal security standards for Member States on strategic and operational levels. It was also mentioned that even though it is not a part of the ENISA mandate the Agency could enhance its communication with the defence sector.

In relation to CSIRTs crisis management some EU Officials stated that ENISA lacks staff and personnel to properly support CSIRTs in a crisis.

5 Operational Perspective – Baseline Capabilities for CSIRTs

As for **baseline capabilities**, ENISA has identified four focus points for its research and continuous work to support CSIRTs. These include ‘mandate and strategy’, ‘service portfolio’, ‘operational capabilities’ and ‘cooperation capabilities’. These baseline capabilities aim to tackle the diversity of capabilities across Member States, which is seen by ENISA as the main obstacle to cross-border cooperation and incident response.

“On organisational and political level, ENISA CERT activities provide a good level of support”

Respondent from a Member State Body

5.1 The road ahead – the ENISA perspective

During the internal ENISA workshop a number of action points for the Agency’s work were brought forward and subsequently included in the survey and interview questions.

5.1.1 Stronger ENISA Voice

To date, ENISA has primarily delivered paper reports, some of which may have lacked sufficiently straightforward recommendations especially to the CSIRT community. This was done deliberately so as to create community buy-in and in order to not be perceived as pushing ideas onto the national and governmental CSIRTs that were in the process of developing and finding their own way.

Nevertheless, ENISA has built a stronger position over the years and should therefore take more of a stance in the papers, studies and public statements that it produces. Instead of limiting papers to stock takings and vague suggestions, it was agreed that ENISA should take a bolder stance and taking more risks in terms of speaking its mind more proactively and directly.

5.1.2 Proactive Endorser

Similar to the prior point, it was pointed out that any kind of support or validation of an initiative, even in the form of a simple endorsement, is important for professionals of the trade. While ENISA at times has preferred to be on stand-by and to wait for requests from the community, it was agreed that the Agency should become more proactive. One participant stated that ENISA should help improve the overall international cooperation by engaging communities and act as a trusted partner that finds sponsors for CSIRTs.

ENISA is able to support some initiatives within the framework of rules for such support. However, instead of supporting initiatives in ‘stand-by mode’ waiting for requests to come, ENISA should be more proactive and not wait for support requests to come. As an example, ENISA could recommend and push open source code on GitHUB[4].

[4] GitHub is a web-based Git repository hosting service, which offers all of the distributed revision control and source code management (SCM) functionality of Git as well as adding its own features. https://github.com/

5.1.3 From paper based studies to service oriented support

As one of the current challenges, support to CSIRTs to build up capabilities with limited resources available at the Member State level was identified. This represents an opportunity for ENISA to take a more active role in supporting the implementation of the baseline capabilities of CSIRTs, which would also be a means to meet the increasing expectations of CSIRTs towards this kind of assistance. From the past experience with the community, it is apparent that CSIRTs appreciate direct interaction and practical advice.

ENISA – CERT Inventory

Inventory of CERT teams and activities in Europe

VERSION 2.16
SEPTEMBER 2015

The shift from paper work to ad hoc support and more tangible advice could be achieved by using a more interactive approach through, for instance, ENISA going onsite upon request to perform a maturity assessment of a CSIRT coupled with an overview of how the team is situated in the community.

Initial requests of this kind have already been received by ENISA (although formally it may fall under Article 14 'Requests to the Agency'[5]), and as such requests are expected to increase in number. As certifications of CSIRTs are on the rise (for instance by the TF-CSIRT Trusted Introducer (TF-CSIRT/TI)[6], which offers registration/listing, accreditation and certification to European CSIRTs.[7]), ENISA is committed to assisting the teams in reaching this status.

It was agreed that ENISA, in addition to its studies, should develop a more service based approach vis-à-vis the CSIRTs, including offering multiple products and services to the CSIRTs.

5.1.4 Two-speed approach to less and more mature CSIRTs

ENISA trainings constitute an important means for improving the baseline capabilities of CSIRTs. However, as the level of maturity of CSIRTs are somewhat uneven, it was suggested that ENISA further tailor its trainings putting, for instance, some of the training activities under the CyberEurope[8] label (e.g.to offer specific trainings that can improve the right skills which will be tested during the CE exercise). Supporting CSIRTs and adapting to differences in maturity of new and less mature teams is seen as a success factor to ENISA. This is an important factor in managing the expectations of CSIRTs.

[5] Regulation (EU) No 526/2013 of the Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004.: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

[6] TF-CSIRT: The Trusted Introducer Service (TI) lists well known teams and accredits as well as certify teams according to their demonstrated and checked level of maturity. https://www.trusted-introducer.org/

[7] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes

[8] Cyber Europe: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe

5.1.5 Materials for the CSIRT Community

In line with the findings of the 2014 Impact Assessment and Roadmap report, ENISA looks to produce handbook type materials for the CSIRT community. The key suggestions include a “CSIRT tool book”, which would focus on what is needed to run a CSIRT, and a playbook on how to deal with different types of incidents.

5.1.6 Benchmarking of baseline capabilities

In view of ensuring a benchmark for the sector, one additional suggestion was for ENISA to declare CSIRT teams as meeting, or even exceeding, the ENISA recommended baseline capabilities. This could be seen as a complement to, or as a first step for CSIRTs towards obtaining the TF-CSIRT Trusted Introducer certification.

National/governmental CERTs
ENISA's recommendations on baseline capabilities
enisa

5.2 Respondent views

Most respondents, and in particular the national and governmental CSIRTs were in favour of ENISA proactively endorsing or supporting initiatives relevant to the CSIRTs and other operational security communities. It was also suggested that if there are initiatives relating to funding for CSIRTs, ENISA should play an active role in supporting the CSIRTs in acquiring funds.

When asked whether ENISA should create a certified list of companies as trusted cybersecurity service providers, the response was mixed. The main question brought forward was whether this type of activity was best done at the EU or Member State level. It was believed that if it was to be done by ENISA, some convincing at the local level would be necessary, although it was clear that some Members States are not sufficiently active in the field. On a positive note, it was seen as putting pressure on the market, which would facilitate the identification of cybersecurity-trusted providers in a domain where many claim to be experts without the actual expertise.

Some respondents expressed the need for ENISA to provide more activities and support for operational baseline capabilities for CSIRTs. Most respondents agreed that ENISA has an important advisory role to play but on the other hand, since ENISA has limited operational mandate, ENISA would not be in a position to assess CSIRTs operational capabilities. Others mentioned that TF-CSIRT is already active in the accreditation scheme and ENISA could assist them in developing it. One National Liaison Officers respondent stated that a CSIRT Baseline Capabilities Assessment could be an additional focus area and activity to be further considered by ENISA.

5.3 Proposed Roadmap to 2020 (based on the 2014 report & 2015 results)

PROPOSED ACTIONS- PILLAR I: BASELINE CAPABILITIES FOR CSIRTS	TIMELINE
Stronger ENISA voice • This action involves ENISA to take a clearer stance in its papers, studies and public statements, towards proactively communicating opinions and recommendations.	Short – medium term

Proactive endorser • Certified list of trusted cybersecurity service providers • Financial support to relevant initiatives:	Short – medium term
Service oriented support (e.g. art. 14 request) • ENISA to develop a more service based approach vis-à-vis the CSIRTs: • Ad hoc requests various services	Medium – long term
Two-speed approach accommodating less and more mature CSIRTs • Tailored trainings/exercises • Materials • Greater focus on technical updates, checklists, summaries	Medium – long term
Materials for CSIRT Community • CSIRT tool book on what is needed to run a CSIRT • Play book – a catalogue for incident handling	Short – medium term
CSIRT baseline capabilities • ENISA assistance for CSIRTs to reach higher level of maturity (e.g. TI certification) • Definition of baseline capabilities instead of stock taking	Short term Long term
Reinforced Information Exchange and Connector Role: • Improved communication and enhanced information sharing • Website – mailing lists – networking and community building	Short – medium term
Awareness raising Enhance the awareness and up-take of ENISA materials (baseline capability) by advertising them more widely, within the CSIRT community and other operational communities	Short – medium term

6 Operational perspective - Capacity building, good practices, and CSIRT training

ENISA's support for CSIRTs in terms of capacity building focuses primarily on trainings, workshops, exercises and dissemination of good practices. In addition, the awareness and perception of Article 14 requests to the Agency was examined following an increase in related workload for ENISA over the past years. In practice requests include support information sharing projects driven by the CSIRT community, various trainings, assistance in enhancing the cybersecurity capabilities and support to specific projects, for instance honeypots.

6.1 The road ahead – the ENISA perspective

During the internal ENISA workshop a number of action points for the Agency's work were brought forward and subsequently included in the survey and interview questions.

6.1.1 Information Exchange and Connector Role

The ENISA view is that the Agency should explore further possibilities to reinforce its role as information exchange connector. While the expectations within the CSIRT community remain quite high, with varied ideas of what could or should be achieved through information sharing. From the ENISA angle, the Agency can serve by sharing information from to relevant stakeholders and by providing guidance on good practices. Thanks to its unique position in the community, ENISA will continue to leverage this advantage to connect community members as well as linking them with relevant players.

The Connecting Europe Facility Cyber Security Digital Service Infrastructure [24] (CEF Cyber Security DSI) is defined in the CEF Annual Work Programme (WP) 2014 and 2015. The preparatory actions foreseen in the CEF WP 2014 (European Commission, 2014b) are aimed at preparing the DSI as a mature DSI for the CEF WP 2015 (European Commission, 2014a) to establish and launch a core cooperation platform and mechanisms that will enhance the EU capability for preparedness, cooperation and information exchange, coordination and response to cyber threats. Such mechanisms will be used by Member States on a voluntary basis, to strengthen capacity building and cooperation, in line with established governance structure and requirements (European Commission, 2014c). ENISA already contributes to this initiative as member of the Governance Board.

6.1.2 Sharing Good Practices among the Teams

ENISA discussed a tool for sharing good practices, which could also mix the features of a blog and a forum, and be used as a social network for the CSIRT community. The existing cyber exercise platform (developed by ENISA) was mentioned as a working example of an information exchange platform, which could be used as a pilot version for exchange between MS in case of crisis. This could be transformed into a platform for dynamic day to day information exchange, as requested by some member States. ENISA should explore the possibility of hosting an informal social network for the operational security community.

6.1.3 Trainings and Train-the-Trainers

To date, trainings have been limited to CSIRT services in the context of baseline capabilities. However, in terms of capacity building, the content of trainings should shift from stand-alone topics to more modular topics to create high value trainings for maturing teams. Therefore, in order to better cater to different maturity levels of the teams, current CSIRT trainings could be further enhanced in order to improve 'training of the trainers' through for example online webinars. In parallel to trainings on "this is how you train people", the Agency would still offer the modular subject matter trainings to support the development of baseline capabilities. This was also seen as a way of better meeting the needs of more mature CSIRTs.

Good Practice Guide on Training Methodologies

How to become an effective and inspirational trainer

6.1.4 Participant Evaluations

In an attempt to better meet the needs of CSIRTs of varied maturity levels, ENISA discussed the possibility of adding assessments of the participants prior to the trainings and exercises. This would ensure a good fit between the level of the participant and the level of difficulty of a training or exercise. It would also be used as a tool to test the new skills acquired at the end of a training session, and implicitly as a motivator for the participants to stay attentive during the training. Furthermore, based on such assessments, ENISA could try to identify the weak points in exercises (e.g. national and European), and propose the development of additional trainings thereby continuing the training lifecycle.

6.2 Respondent views

The respondent views for ENISA capacity building, good practices, and CSIRT training complement the views expressed in the internal ENISA workshop, with the expectation that no mention was made of participant evaluations or the re-using of training materials.

Various respondents believe that ENISA should focus on information sharing by putting into place effective mechanisms to cement their information sharing (threat intelligence, incidents, etc.) and connector role. Respondents mentioned that this could be done through a secure communications platform and/or working with Internet Service Providers. One Governmental CSIRT mentioned that ENISA should focus on establishing additional information security exchanges in different sectors such as the healthcare or energy sector. Moreover, respondents mentioned that at the moment, information is shared mainly via conference calls which remains inefficient and that more face to face meetings would benefit the community as a whole.

Guideline on Threats and Assets

Technical guidance on threats and assets in Article 13a

The vast majority of respondents agree that ENISA has been successful in disseminating good practices to relevant operational security community. In addition, many respondents brought up the point that these ENISA activities, security guidelines and procedures are used and applied to their teams, stressing that ENISA is an ”influential player in the development of international sharing of cyber information." Furthermore, one non-EU CSIRT stated that ‘ENISA material is excellent for the construction of the CSIRTs and has helped many times with controversial moments.’

All respondents mentioned that more trainings should be provided to the trainers of the CSIRT community, especially training for teams that are, or will be, newly created. One respondent stated that ENISA should organise a ”Senior Manager Workshop” to support CSIRT leaders to effectively manage, train and provide leadership to their teams and the greater CSIRT community. Moreover, a few respondents mentioned that ENISA could bring those trainings to MSs in order to avoid costly travel.

To conclude, most respondents believe that ENISA should continue working as a facilitator, coordinator and a trusted introducer, disseminating good practices and bringing people together while not enter into an operational role.

6.3 - Proposed Roadmap to 2020 (based on the 2014 report & 2015 results)

PROPOSED ACTIONS –PILLAR II: CAPACITY BUILDING, SHARING GOOD PRACTICES AND CSIRT TRAINING	TIMELINE
Reinforced Information Exchange and Connector Role: • Improved information exchange (threat intelligence, incidents, etc.) and enhanced sharing of good practices • Website – networking and community building	Short – medium term
Continued support for mature CSIRTs • Regular updates of CSIRT capacity building material a clearer focus on “advanced team support” for mature CSIRTs • Greater focus on technical updates, checklists, summaries	Medium – long term
Clearer focus on operational vs strategic reports: • More technical reports for practitioners • Policy-related reports for decision makers	Short – medium term
Trainings • Train the trainer • Module subject matter trainings. • Participant evaluations- pre/post trainings and & exercises	Medium – long term

Re-use of training material as a step to streamline the services of the team following the reorganisation	
Awareness raising Enhance the awareness and up-take of ENISA materials (capacity building) by advertising them more widely, within the CSIRT community and other operational communities	Short – medium term

7 Operational perspective - Support CSIRTs to better collaborate with Law Enforcement Agencies

In 2010, ENISA started its support for operational collaboration between the CSIRTs and LEAs (law enforcement agencies). Various activities have since been launched, including stock-takings of legal and operational obstacles that prevent collaboration, advice resulting from that, workshops that brought together members of both communities, consultation with members of both communities, etc.

7.1 The road ahead – the ENISA perspective

During the internal ENISA workshop a number of action points for the Agency's work were brought forward and subsequently included in the survey and interview questions.

7.1.1 ENISA-EUROPOL collaboration

> "ENISA should bridge the gap between CERTs and Law Enforcement by further collaborating with the European Cybercrime Centre (EC3) at Europol and Eurojust."
>
> Respondent for the public sector

7.1.1.1 Workshops

Despite a slow start, the ENISA collaboration with European Cybercrime Centre (EC3) at Europol on organising workshops has over time become an established practice[9] [10] [11] and many participants have expressed their interest to continue with these kinds of workshops. The focus should be to make sure that CSIRTs, in the first place, are equipped to interact with law enforcement agencies. While LEA's main objective is to collect evidence and arrest perpetrators, they tend to be less interested in learning new techniques. Nevertheless, in the context of botnet takedowns, there are examples of direct communication between EC3 and CSIRT teams, especially when cases are being investigated during CSIRT/LEA workshops. This is a good example of an area where ENISA could solidify its role while continuously exploring together with EC3 additional needs of the CSIRTs and LEA community.

7.1.1.2 Good practice library for CSIRTs and LEA cooperation

In this vein, the current ENISA/EC3 current taxonomy project should be further elaborated. There should be two focus points in relation to the taxonomy related work. Firstly, improved LEA-CSIRT cooperation in the fight against cybercrime. Secondly, strategic cooperation with EC3 that would go beyond the current ENISA/EC3 workshops and the "Report on information sharing and common taxonomies between CSIRTs and Law Enforcement" project.

[9] 4th ENISA/EC3 Workshop: https://www.enisa.europa.eu/activities/cert/events/4th-enisa-ec3-workshop

[10] 8th CERT workshop - Part II (co-organised with EC3): https://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-ii

[11] 9th CERT ENISA/EC3 Workshop Part II: https://www.enisa.europa.eu/activities/cert/events/9th-cert-workshop-part-ii

7.1.1.3 Digital Forensics

Law enforcement agencies are by nature typically restrictive in the exchange of evidence. Nevertheless, in order to solve cases, players from different countries should be involved, which opens a door for ENISA to assist in the process related to digital forensics. For instance, ENISA could further approach the operational level of LEAs in order to develop training scenarios where it would be able to bring its expertise on subjects such as how to exchange information securely using Pretty Good Privacy (PGP) or how to take forensics samples from a procedural point of view.

Network Forensics

Handbook, Document for teachers

7.1.1.4 ENISA as Europol observer

Even though fighting cybercrime is not its mandate, many communities look to ENISA for guidance. Therefore, ENISA could work more closely with EC3 on operational activities, for example, as an observer Through an observer status, ENISA could gain knowledge, for instance on how handle botnets, while bringing technical expertise to the EC3, which would ensure a mutually beneficial collaboration between the two Agencies.

7.1.2 LEA – CSIRT collaboration activities

7.1.2.1 CEPOL – trainings/networking

Whilst ENISA has organised joint LEA/CSIRT trainings[12] [13], it should also look into the possibility of collaborating with the European Police College[14] (CEPOL). There is added value of bringing CSIRT expertise into the law enforcement community as police and CSIRTs are interested in similar topics, such as taking down botnets, handling incidents, etc. In many cases LEAs outsource technical work to CSIRTs providing a clear link between the organisations, which can be built upon.

Another idea in this area is for ENISA to engage prosecutors or at least raise their awareness about activities in the CSIRT world. Similarly, awareness about prosecution phases should be raised for CSIRTs. However, for the latter case ENISA is less qualified as it has limited knowledge on how the police operates.

7.1.2.2 Guidance to CSIRTs on H2020 funding

Another topic that was discussed is the EU Framework Programme for Research and Innovation[15], also known as "Horizon 2020". A participant mentioned that there are calls about joint collaboration between CSIRTs and LEAs that promote joint exercise to simulate cooperation. Here, ENISA could encourage CSIRTs

[12] Cooperation with Law Enforcement Agencies - Advising in Cyber Crime Cases: https://www.enisa.europa.eu/activities/cert/training/training-resources/legal-cooperation#writing-security-advisories

[13] Cooperation in the Area of Cybercrime: https://www.enisa.europa.eu/activities/cert/training/training-resources/legal-cooperation#cooperation-in-the-area-of-cybercrime

[14] The European Police College (CEPOL) is an EU agency dedicated to providing training and learning opportunities to senior police officers on issues vital to the security of the European Union and its citizens: https://www.cepol.europa.eu/

[15] The EU Framework Programme for Research and Innovation: https://ec.europa.eu/programmes/horizon2020/

or LEAs to participate in calls to get funding through grants by coaching and providing guidance. In fact, it seems many CSIRTs and LEAs want to participate in such calls but have no idea what the Commission might be looking for.

7.2 Respondent views

When asked whether cooperation between ENISA and EC3 should go beyond the current ENISA/EC3 workshops and if both organisations should be more involved at the level of operational cooperation, the response was mixed. For some respondents it seemed obvious that ENISA should bridge the gap between CSIRTs and law enforcement by further collaborating with the EC3 and even with Eurojust. Others disagreed, claiming that ENISA should stick to technical aspects and not go into, for instance, forensics as this topic could be too politically touchy.

One respondent from a law enforcement agency summed up the current situation and needs in the following way: ‘Not only is cybercrime borderless, it also moves seamlessly from one sector to another’. Nobody wins if they try to solve the issues on their own without sharing information on what is going on. However, information sharing requires trust as a lot is at stake. For instance, a bank runs a huge reputational risk if its clients learn about cyber-attacks affecting their bank accounts, and hence will be reluctant to share information about security issues. However, ‘by not sharing information, you cannot learn from others’, as one respondent stated. By teaming up in public-private partnerships (PPP), for instance, banks and financial institutions in partnership with law enforcement, trust can be built and information shared which benefit all parties. In this context, ENISA could develop a framework on how information can be shared, what information can be shared (overcoming national privacy laws) and with whom. By doing this, ENISA would raise its profile among LEAs and make a valuable contribution. The idea of ENISA expanding its scope and developing PPPs (academia, National and Governmental CSIRTs, Eurojust and registry services, etc.) was echoed by another respondent.

Some additional concrete examples of possible trainings included to mainstream the topic of cybercrime in the general curricula. The respondent claimed that a lot of cooperation stays at a high (abstract) level of organisations when it actually needs to focus on the operational levels. By this, the respondent meant that trainings needs to reach further than just a few specialists, otherwise, the gaps in skills set will be too wide within organisations. Very often, only one person from each organisation is sent to a training, when in reality, the awareness needs to be broader, including all levels of the organisation from the local police officers to the specialised units. More workshops and trainings on forensics would be good as well as training of colleagues on the police force about the dark net and how it is used by criminals for information sharing. Respondents were in favour of ENISA collaborating with CEPOL to organise joint LEA/CSIRT trainings.

Cooperation with Law Enforcement Agencies - Advising in Cyber Crime Cases

Toolset, Document for students

A majority of the respondents were positive to the idea of ENISA supporting (through coordination and guidance) CSIRTs/operational security communities on how to participate in Horizon 2020 calls to obtain additional funding. One National CSIRT affirmed that ENISA could support initiatives relating to funding for CSIRTs. Another respondent stated that often there are situations were different teams are working on the same solutions and sometimes common projects with small funding can make a big difference. ENISA could assist different teams from different countries to work together, using joint resources instead of each CSIRT going for it alone.

7.3 Proposed Roadmap to 2020 (based on 2014 report & 2015 results)

PROPOSED ACTIONS –PILLAR III: CSIRT SUPPORT CSIRTS TO BETTER COLLABORATE WITH LAW ENFORCEMENT AGENCIES	TIMELINE
ENISA – EUROPOL collaboration • Joint workshops • ENISA observer status and knowledge transfer	Short – medium term
Good practice library for CSIRTs and LEAs • Taxonomy report • Fight against cybercrime	Short – medium term
Facilitate more joint CSIRT-LEA events and training • Mainstream the topic of cybercrime in the general curricula • Additional workshops and trainings on forensics and the dark net	Short – medium term
Digital forensics – knowledge sharing	Short – medium term
Enhanced support to the fight against cybercrime • ENISA to explore possibility of LEAs to enter into public-private partnerships (PPP) • ENISA could develop an information sharing framework	Short – long term
LEA-CSIRT collaboration activities • CEPOL trainings/networking • Guidance to CSIRTs on H2020 funding	Short – medium term
Awareness raising Enhance the awareness and up-take of ENISA materials (CSIRT-LEA) by advertising them more widely, within the CSIRT community / other operational communities & LEAs	Short – medium term

8 Operational perspective Cyber crisis cooperation and exercises

ENISA has been a facilitator for EU Member States by supporting the exchange of good practices in the area of Cyber Crisis Cooperation and Exercises through a series of pan-European cyber exercises such as Cyber Europe and Cyber Atlantic. In addition, ENISA published a 'Good Practice Guide on National Exercises' with the aim to assist European stakeholders to design, plan, execute and monitor a national exercise on the resilience of public communication networks. Finally, ENISA is organising annual international conferences covering topics in the area of cyber crisis cooperation and exercises.

8.1 Cyber Crisis Cooperation and Management

ENISA's work package for 2015 focuses on cyber crisis cooperation and management in the following topics:

- Pan-European cyber exercises management (Cyber Europe and EuroSOPEx);
- Enhance the capacity to support and organise cyber exercises;
- Promote maintain and improve EU cyber crisis cooperation plans and procedures (e.g., EU SOPs), which includes bringing closer the cyber crisis cooperation community.

This work package focuses on ENISA further enhancing its methodology, training outreach and technical capability to organise large-scale cyber crisis exercises in addition to seeking to facilitate the planning of the next pan European Cyber Exercise in 2015-2016.

8.2 The road ahead – the ENISA perspective

During the internal ENISA workshop a number of action points for the Agency's work were brought forward and subsequently included in the survey and interview questions.

8.2.1 Cyber Crisis Management and Contingency Planning

ENISA has developed a good practice guide on national risk assessment and offers regular trainings on the topic. Additionally, ENISA has led a study on cybersecurity crisis management and is currently leading a study on general crisis management. ENISA should be able to offer a training on the latter by 2016.

8.2.2 EU-Level NIS Cooperation (EU-SOPs)

The EU-SOPs (Standard Operating Procedures) give guidance on how to manage major cyber incidents that would escalate to a crisis. ENISA has been and will remain heavily involved in the development of the EU-SOPs.

> "ENISA should have a key role in preparedness measures for cyber crisis management."
>
> One National Liaison Officer respondent

As the EU-SOPs will evolve in the context of the NIS Directive, potential cooperation between the teams within ENISA can be sought. First, it was identified in Cyber Europe 2014 that the EU-SOPs should include procedures for technical cooperation for incident handling (currently it contains only operational cooperation procedures for crisis management.

Second, a Commission initiative under the Connecting Europe Facility (CEF) cybersecurity pillar currently looks at the possibility of building on existing tools and capabilities, for further developing of a common platform for Member States to cooperate during cybersecurity incidents, crises and to exchange relevant information on a trust basis. ENISA's experience in fostering cooperation during simulated cyber crises will be valuable for this CEF initiative promoted by the Commission. In this context, ENISA should play a relevant role.

8.3 Cyber Exercises

Cyber Cooperation and Exercises

NLO Meeting, 04 March 2015, Athens

8.3.1 Pan European Cyber Exercises (Cyber Europe series)

ENISA will continue organising the Cyber Europe series every two years while developing new exercising opportunities on a more regular basis. Synergies within ENISA can be sought with regards to exercises and trainings: future technical exercises should reference related trainings offered by ENISA and vice versa.

8.3.2 Supporting other Cyber Exercises

ENISA has developed a Cyber Exercise Platform to support the planning and execution of Cyber Europe exercises. This platform will be opened in 2016 to Member States so that they can use it to plan and execute their own exercises.

8.4 Respondent views

One EU Official stated that ENISA is trying its best given the size of the organisation and considering that the bar is getting raised by the digital Commissioners. On the subject of cyber crises management, the same respondent argued that in a moment of crisis cooperation is key and it allows for things to be accomplished faster. Unfortunately, CSIRTs have a limited view on what is going on beyond their own field and there is a disconnection between the local (MS) and central (EU) levels. They know their national competence, like in the case of the Icelandic volcano eruption where Eurocontrol [25] played a crucial role as a pan-European player. Still EU MSs do not act and it seems that a cyber-crisis is needed for them to take action on crisis coordination. What is needed is an EU-level framework for crisis management within the cyber sector.

Respondents from various stakeholder groups agreed that the Cyber Europe exercises help develop practical cooperation between different stakeholders during cross-border incidents. As one CSIRT respondent put it: 'They help foster trust building and building of relations'. The relationship building extended, in some cases, beyond the stakeholders of the national or governmental CSIRT, and allowed for further development of practical cooperation in-country.

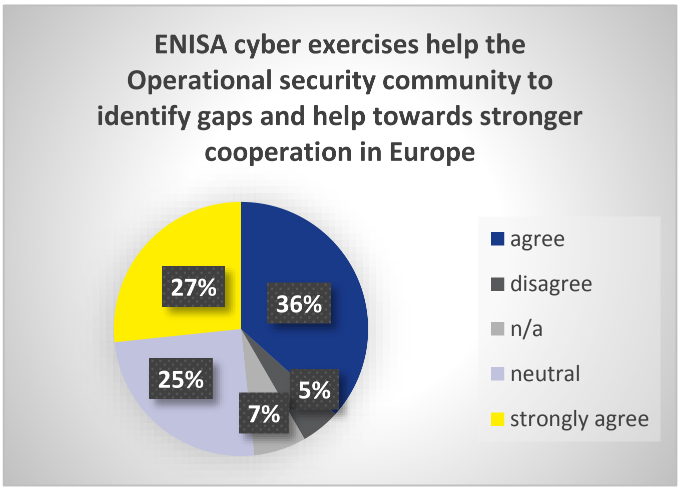
The ENISA cyber exercises, including the Cyber Europe series, were also considered to help the operational security community, including CSIRTs, to identify gaps and help towards stronger cooperation in Europe. However, while respondents from most stakeholder groups agreed to this statement, one respondent pointed out that *'when it comes to gaps, on paper, the official procedures for contacting CSIRTs is good but* *in reality you contact those you know. Thus, gaps in developing personal relations still exist. Nonetheless, having the official contacts is important and used as a fall-back mechanism'.*

Respondents saw the ENISA cyber exercise material as relevant and useful to operational security professionals, in particular from the Member State bodies, especially the SOPs. However, as one respondent pointed out, if a crisis occurs, not all Member States were likely to follow the SOPs as these are not mandatory and ENISA has to rely on the good will of the Member States. Therefore, the use of the procedures should be made, if possible, mandatory.

> "The Cyber Europe series is very useful and important as it helps to fill the gaps and study new technical challenges."
>
> Respondent from a Member State body

Feedback on the ENISA Cyber Europe exercises can be summarised in the following themes:

- **Content**: Both respondents from the national and governmental CSIRT community and EU official stated that the Cyber Europe Exercises could be more technical in their nature. This may include more advanced technical challenges (i.e. test effect of APTs to organisations (detection, reaction, prevention) and more collaboration on the crisis management level. In addition to having more topics on privacy and cloud computing and more international industry generic and specific exercises, including red teaming and force on force. One of the respondents went as far as to say that while the Cyber Exercises do satisfy the political agenda in Europe and show that things are being done in the cyber domain, it would serve more purpose to steer away from the politics and go deeper into the technical, practical and realistic aspects of the cyber world. The current scenarios presented by ENISA were perceived as highly tailored to the political level and while they are well-prepared they should focus more on technical aspects. The same respondent stressed that the NATO exercises, although a bit too 'military', were good examples of great exercises as they are more practical and realistic.



- **Frequency**: For some respondents, it was also preferable to increase the frequency of the Cyber Europe Exercises from every second year to twice a year, even though this would make it harder for the participants to find funding for, it would be more beneficial.
- **Scope**: It was seen as a positive development that the Cyber Europe Exercises are extending their reach to include the private sector. CSIRTs were believed to benefit from engaging more with the private sector since, for the most part, if/when something happens it happens in the private sector, and in many cases the private sector holds more critical resources and information.

- **Geography**: With regards to the issue involving the growing size of participants in Cyber Europe exercises, regional exercises could be considered, according to a respondent from a national CSIRT. For example, a Baltic Nordic Regional exercise or grouping could be used as a test case. The idea of regional grouping was also brought forward by an EU official who claimed that the Cyber Exercises would be better suited to tailor to a smaller audience based more on regional boundaries. The reason for this, according to the respondent, was that in a real cyber crisis, the situation looks a lot different. Entities handle incidents locally and regionally and very rarely on such as scale as the ENISA Cyber Exercises.
- **Results**: One respondent pointed out that following an exercise, the outcomes disseminated by ENISA were very generalised and politically correct, when, in reality, the participants were keen on learning the exact outcomes on how specific teams/individuals performed, for instance in a possible comparison or ranking scheme. This was echoed by an EU official interested in raising awareness at the political level who suggested that the feedback received from the exercises could be better disseminated and spread to persons who were more difficult to reach, or individuals, entities that did not participate in the exercises.
- Improved means of **information sharing** was stressed by several stakeholders who urged ENISA to also disseminate the feedback from the exercises to people who were not able to attend. ENISA was also requested to put in place effective mechanisms for information sharing and not limit it to conference calls.

When asked about additional CSIRT focused areas and activities to be covered during Cyber Europe exercises, the respondents provided several suggestions, including:

- **Increased technical focus:** More on data protection, on social media and about Internet infrastructure and Cyber Supply Chain. More on developing European Cyber capabilities, such as a European search engine, and on cultivating European cyber independence in the face of firmware, hardware or computers are made in China and the US – not Europe.
- **Including the political level:** One respondent stressed the importance of linking cyber to the EU political level by building on the cyber scenario. This would allow the ministries and politicians to understand the cyber domain better and, conversely, the technical experts would better understand the political level

8.5 Proposed Roadmap to 2020 (2015 results)

PROPOSED ACTIONS- PILLAR IV: CYBER CRISIS COOPERATION AND EXERCISES	TIMELINE
EU-level Cyber Crisis Cooperation • Cyber crisis training with a pan-European focus • Elaboration of EU-level SOP • Involvement in the development of a MS platform for cooperation during cybersecurity incidents	Short – long term
Cyber Exercises	Short – long term

• Continued implementation of Cyber Europe series (bi-annual): sharper technical focus and regional groups. Enhanced feedback mechanism. • Support to other cyber exercise though the Cyber Exercise Platform	

9 Conclusions and Road to 2020

Chapter 9 discusses the main findings from both the 2014 and the current study and concludes the impact assessment of ENISA CSIRT support activities by proposing a roadmap for future activities of ENISA till 2020.

9.1 360° feedback

As mentioned in the description of the methodology of this study, a structured approach was employed during the interviews in order to allow for the respondents to freely and anonymously express their views on ENISA's support to the CSIRT community. However, much of the feedback was not directly linked to the ENISA four activity pillars focused on CSIRTs. Hence, this chapter starts off by capturing a number of respondent views to provide a 360° understanding of the possible future direction of ENISA.

9.1.1 Expanded constituency

Overall, the respondent views and findings concur with the findings of the 2014 report. ENISA is still considered to be the representative voice of the European CSIRT community and of other operational communities. Several respondents even pointed to the possibility for ENISA to expand its constituency (working increasingly with CSIRTs in various sectors) and coverage beyond the borders of the EU. For instance, there was a call for ENISA to enhance communication with non-EU countries and to establish minimal security standards for Member States on strategic and operational levels.

9.1.2 European cyber independence

Echoing the words of Commissioner Oettinger, one respondent called for a stronger mandate that would allow ENISA to drive the EU's technological independence. ENISA has a real possibility of becoming instrumental in the EU's ambition to regain 'digital sovereignty" and to reassert its digital independence. This new branch of strategic activities would examine the 'bigger picture', including industrial politics, and provide input in the form of strategic studies and workshops.

As an extension of this reasoning it was suggested, that ENISA should focus more on cybersecurity aspects of industry, social networks and data protection related issues. This could include and in-depth look into the actual cyber threats and impacts related to industry, as well as social networks.

9.2 Discussion on key findings

9.2.1 Facilitator and connector role

The respondents attest to a strong support of ENISA's role as the facilitator and coordinator of the CSIRT community, as well as a middle ground mediator between the CSIRTs and the Commission. ENISA bridges the gap between the technical focus of the CSIRTs and the policy focus of the Commission.

ENISA should also strengthen the ties between the CSIRTs and LEAs through further collaborating with the European Cybercrime Centre at Europol, Eurojust and CEPOL.

In addition, ENISA should expand its reach and scope and develop private-public partnerships (academia, other non-governmental CSIRTs, and registry services).

9.2.2 Focus and develop further exercises and workshops

ENISA has a key role in supporting the CSIRT and other operational communities through its pertinent and state of the art workshops and exercises. With regards to Cyber Europe exercises, we received different suggestions such as focusing the exercises more on crisis management. These include more advanced technical challenges to the exercises, and to accommodate the growing size of participants by grouping them regionally, while also inviting participations from the private sector. A point for improvement is the information sharing following an exercise in order for the individual teams and participants to be able to compare levels of expertise, results, etc.

9.2.3 Putting new topics on the agenda

Being uniquely positioned in the cybersecurity landscape, the CSIRT community welcomes the Agency to make use of its experience and to push the envelope by being bolder and taking a clearer stance on in its publications and to proactively reaching out and endorsing initiatives when identifying them. While the materials pertaining to the baseline capabilities (pillar I) and capacity building (pillar II) remain vital contributions to the community, there is also scope for a sharper technical focus of the ENISA reports, on the one hand and more policy oriented reports on the other.

It was also suggested that ENISA uses its unique position to bring 'new' topics and trends or important developments in the sector forward. For instance, ENISA could engage in discussions on topics such as network neutrality, acceptable traffic management and security, including levels of incident protection allowed. This could be done through short 'viewpoints' or white papers, which can be produced within a short time frame, requiring less effort than the typical ENISA studies.

ENISA should find multipliers to ensure that the important work done by its teams reaches even further, beyond the established communities. Repeatedly the "modest" size and strongly limited budget of the Agency was highlighted as biggest obstacle for the agency to perform up to all expectations.

9.3 The Way Ahead: roadmap for ENISA CSIRT Support

The proposed high-level roadmap 2020 presented below provides an overview of possible areas of priority on the basis of previous chapters.

LEGISLATIVE & REGULATORY: PROPOSED ACTIONS	DEPENDENCIES	TIMELINE
EU Policy of Critical Information Infrastructure Protection (CIIP) • Carry out pan-European exercises, in line with the approach taken in the past: ENISA has carried out Cyber Europe Exercises in 2010, 2012 and 2014 and will continue to do so in 2016. • Adopt a minimum set of baseline capabilities and services and related policy recommendations for (CSIRTs) to function effectively, in particular with regards to the CIIP: ENISA already established various baseline capabilities and services for CSIRTs (capability guidance materials, technical updates, improved communication, enhanced information sharing, etc.)	N/A	Short term
Proposed NIS Directive[16] The Commission would ask ENISA to: • Assist in the operation of the cooperation network; • Provide MS and the EU with expertise and advice; • Facilitate the exchange of best practices.	Adoption of the proposed NIS Directive	Short – medium term
ENISA Annual Work Programme 2015 • Short- and mid-term sharing of information regarding issues in NIS; • Assist in public sector capacity building; • Support for EU cooperation initiatives amongst NIS-related communities in the context of the EU Cyber Security Strategy (EU CSS); • European cyber crisis cooperation through exercises.	Ongoing work	Short term

[16] At the time of writing, adoption of the NIS Directive is pending. However, no significant changes are expected to the proposed directive.

PROPOSED ACTIONS - PILLAR I: BASELINE CAPABILITIES FOR CSIRTS	DEPENDENCIES	TIMELINE
Stronger ENISA voice • ENISA to take a clearer stance in its papers, studies and public statements, towards proactively communicating opinions and recommendations.	N/A	Short term
Proactive endorser • Facilitate a compilation of an EU-wide certified list of trusted cybersecurity service providers; • Pro-active support and/or endorsement to relevant initiatives: ENISA should proactively support initiatives and act as a trusted partner that finds sponsors for CSIRTs. Endorsement from the Agency would provide a boost to key initiatives.	Support / requests from national level entities (CSIRTs and other operational communities)	Short – medium term
Service oriented support (e.g. Art. 14) • ENISA to develop a more service-based approach vis-à-vis the CSIRTs: Services portfolio to include, but not be limited to, CSIRT maturity assessments; • Ad hoc requests for various services coming from the community to ENISA should be encouraged.	Requests from national level entities (CSIRTs and other operational communities)	Medium – long term
Two-speed approach accommodating less and respectively more mature CSIRTs • Tailored trainings/exercises; • Materials: regular updates of CSIRT baseline capability materials with special attention to the two-speed reality of CSIRT maturity; • Greater focus on technical updates, checklists, summaries.	Insights to existing maturity levels and needs with regard to baseline capability building	Medium – long term
Materials for CSIRT community • CSIRT tool book on what is needed to run a CSIRT; • Play book – a catalogue for incident handling.	Feedback and support from CSIRTs/other operational communities	Short – medium term
CSIRT baseline capabilities • ENISA assistance for CSIRTs to reach next level of maturity ENISA to assess and confirm whether CSIRT teams are meeting, or even exceeding, the ENISA recommended baseline capabilities. Can be seen as a complement to, or as a first step for CSIRTs towards obtaining the TF-CSIRT Trusted Introducer certification. • Helping CSIRTs in effective establishing of baseline capabilities instead of only stock taking of their status.	Requests from national level entities (CSIRTs and other operational communities)	Short term Long term

PROPOSED ACTIONS - PILLAR I: BASELINE CAPABILITIES FOR CSIRTS	DEPENDENCIES	TIMELINE
Reinforced information exchange and connector role: • Improved communication and enhanced information sharing; • Website – mailing lists – networking and community building actions.	Up to date information and feedback from the CSIRTs and other operational communities	Short – medium term
Awareness raising Enhance the awareness and up-take of ENISA materials (baseline capability) by advertising them more widely within the CSIRT community and other operational communities, and by explaining the value they bring: • Key publications • Trainings • Events • Clarification of ENISA role vis-a vis CSIRT community	Up to date information and feedback from the CSIRTs and other operational communities	Short – medium term

PROPOSED ACTIONS – PILLAR II: CAPACITY BUILDING, SHARING GOOD PRACTICES AND CSIRT TRAINING	DEPENDENCIES	TIMELINE
Reinforced Information Exchange and Connector Role: • Further facilitate an improved information exchange (threat intelligence, incidents, etc.) and enhanced sharing of good practices: ➢ ENISA to explore the possibility of hosting an informal social network for the operational security community; ➢ ENISA to explore expanded information security exchange to encompass additional sectors, such as the healthcare, energy, etc. • ENISA own website – networking and community building: as a vital tool for information dissemination, the ENISA website can be revised to improve user interface and intuitiveness.	Up to date information and feedback from the CSIRTs and other operational communities	Short – medium term
Continued support for mature CSIRTs • Regular updates of CSIRT capacity building material a clearer focus on "advanced team support" for mature CSIRTs; • Greater focus on technical updates, checklists, summaries.	Acceptance and support from CSIRTs and other operational communities	Medium – long term
Clearer focus on operational vs. strategic reports: • More technical reports for practitioners; • Policy-related reports for decision makers.	Up to date information and feedback from the CSIRTs and other operational communities	Short – medium term
Trainings • Train the trainer – for more mature CSIRTs to further develop staff; • Module subject matter trainings – development of baseline capabilities: ENISA should develop a 'Senior Manager Workshop' to support CSIRT leaders to effectively manage, train and provide leadership to their teams and the greater CSIRT community; • Participant evaluations- pre/post trainings and & exercises; • Re-use of training material as a step to streamline the services of the team following the reorganisation	Anticipation of future challenges and skills set needs among the CSIRTs and other operational communities	Medium – long term
Awareness raising (similar with awareness action of Pillar I)	Up to date information and feedback from the	Short – medium term

PROPOSED ACTIONS – PILLAR II: CAPACITY BUILDING, SHARING GOOD PRACTICES AND CSIRT TRAINING	DEPENDENCIES	TIMELINE
Enhance the awareness and up-take of ENISA materials (capacity building) by advertising them more widely, within the CSIRT community and other operational communities, and by explaining the value they bring: • Key publications • Trainings • Events • Clarification of ENISA role vis-a vis CSIRT community	CSIRTs and other operational communities	

PROPOSED ACTIONS –PILLAR III: CSIRT SUPPORT CSIRTS TO BETTER COLLABORATE WITH LAW ENFORCEMENT AGENCIES	DEPENDENCIES	TIMELINE
ENISA – EUROPOL collaboration • Joint workshops: ENISA to explore additional topics and challenges to build the workshops on; • ENISA observer status and knowledge transfer: ENISA should work more closely with EC3 on operational activities to gain necessary knowledge.	Anticipation of future challenges and skills set needs among the CSIRTs/other operational communities & the LEAs	Short – medium term
Good practice library for CSIRTs and LEAs • Taxonomy report dissemination and further elaboration; • Further alignment with key actors involved in the fight against cybercrime – for enriching the existing good practices for CSIRTs.	Anticipation of future challenges and skills set needs among the CSIRTs/other operational communities & the LEAs	Short – medium term
Facilitate an additional number of joint CSIRT-LEA events and training • Mainstream the topic of cybercrime in the general curricula and include all levels of the organisation from the local police officers to the specialised units; • Additional workshops and trainings on cyber forensics, the dark net and how it is used by criminals for information sharing and other malicious purposes.	Anticipation of future challenges and skills set needs among the CSIRTs/other operational communities & the LEAs	Short – medium term
Digital forensics – knowledge sharing • ENISA to explore, with the operational levels of LEAs, the possibility to develop training scenarios where they would be able to bring their expertise on subjects such as how to exchange information securely using Pretty Good Privacy (PGP) or how to take forensics samples from a procedural point of view.	Anticipation of future challenges and skills set needs among the CSIRTs/other operational communities & the LEAs	Short – medium term
Enhanced support to the fight against cybercrime • ENISA to explore possibility of LEAs to enter into public-private partnerships (PPP) with relevant actors from various sectors to build trust (a major impediment) and enable increased information sharing. • ENISA could develop a framework on how information can be shared, what information that can be shared (overcoming national privacy laws) and with whom.	Acceptance and support from CSIRTs/other operational communities & the LEAs	Short – long term

PROPOSED ACTIONS –PILLAR III: CSIRT SUPPORT CSIRTS TO BETTER COLLABORATE WITH LAW ENFORCEMENT AGENCIES	DEPENDENCIES	TIMELINE
LEA-CSIRT collaboration activities • CEPOL trainings/networking: ENISA to explore the best way of bringing CSIRT expertise into LEA community, specifically topics such as taking down botnets, handling incidents, etc. In cases LEAs outsource technical work to CSIRTs providing a clear link between organisations, which can be built upon; • Guidance to CSIRTs on H2020 funding.	Up to date information and feedback from the CSIRTs/other operational communities & the LEAs	Short – medium term
Awareness raising (similar with awareness action of Pillar I & II) Enhance the awareness and up-take of ENISA materials (CSIRT-LEA) by advertising them more widely, within the CSIRT community / other operational communities & LEAs, and by explaining the value they bring: • Key publications • Trainings • Events • Clarification of ENISA role vis-a vis CSIRT community.	Up to date information and feedback from the CSIRTs/other operational communities & the LEAs	Short – medium term

PROPOSED ACTIONS- PILLAR IV: CYBER CRISIS COOPERATION AND EXERCISES	DEPENDENCIES	TIMELINE
EU-level Cyber Crisis Cooperation • Cyber crisis training with a pan-European focus: Training on crisis management to be developed • Elaboration of EU-level SOP: ENISA to further develop the EU-SOPs. • Involvement in the development of a MS platform for cooperation during cybersecurity incidents	Adoption of the NIS Directive (EU-SOPs) & decision on CEF cyber platform	Short – long term
Cyber Exercises • Continued implementation of Cyber Europe series (bi-annual): ENISA to explore features such as a sharper technical focus, frequency and scope and regional groups, incl. enhanced feedback mechanism; • Support to other cyber exercises though the Cyber Exercise Platform.	Up to date information and feedback from the CSIRTs and other operational communities	Short – long term

PROPOSED ACTIONS- 360° FEEDBACK	DEPENDENCIES	TIMELINE
Expanded constituency for CSIRT support • ENISA to explore further possibilities to work with and to support CSIRTs in various sectors (private sector, academia, etc.); • ENISA to enhance communication with non-EU CSIRTs and to establish minimal security standards for Member States on strategic and operational levels.	Acceptance and support from CSIRTs and other operational communities. Agreement with/ request from with non-EU CSIRTs	Short terms Medium– long term
European cyber independence • ENISA to explore actions related to strategic digital independence, incl. analysis of industrial politicies, and provide input in the form of strategic studies and workshops; • ENISA to further examine cybersecurity aspects of industry, social networks and data protection related issues.	Up to date information and feedback from the relevant EU institutions and related bodies, CSIRTs and other operational communities	Short – long term

Annex A: List of Interview Questions

	QUESTIONS
1.	To what extent do you agree with the following statement? “ENISA has successfully implemented the Operational Security activities, i.e., CERT support and Cyber Crisis Cooperation and Exercises related activities set out in the Annual Work Programs, in the past five (5) years.”
2.	To what extent you do consider that ENISA was successful in its mission of supporting the national / governmental CERTs at both the operational and policy level?
3.	To what extent are ENISA Operational security activities important in supporting the Cybersecurity Strategy of the European Union, in particular the goals related to co-ordination between NIS competent authorities, CERTs, law enforcement and defence?
4.	To what extent do you agree with the following statement? “ENISA has been successful in disseminating good practices to relevant operational security community stakeholders.”
5.	To what extent do you agree with the following statement? “ENISA has been successful in achieving the objectives outlined in the ENISA Regulation in relation to support to Operational security community in EU Member States.”
6.	How well do ENISA Operational security community activities support the implementation of applicable/relevant EU or national regulations?
7.	To what extent do you agree with the following statement? “ENISA has achieved its objective to develop relationships and enhance Operational security community -related cooperation with EU institutions and bodies.”
8.	To what extent do you agree with the following statement? “ENISA has made a significant contribution in relation to the cooperation with and support to national CERTs (for instance, set-up of CERTs and organisation of cyber exercises).”
9.	Concerning the current focus areas and activities of ENISA, in the area of CERTs and operational communities, what could be additional focus areas and activities to be further considered by ENISA in line with the Cybersecurity Strategy of the EU, and/or beyond for coming five (5) years?
10.	To what extend have the ENISA cyber exercises, including the Cyber Europe series, helped the Operational security community, including CERTs, to identify gaps and help towards stronger cooperation in Europe?
11.	To what extent do you agree with the following statement? “ENISA has contributed to enhancing national CERTs crisis management capabilities”
12.	In the case of a large-scale cybersecurity incident affecting European Member States, how would you expect ENISA to contribute if called upon?
13.	To what extent do you agree with the following statement? “ENISA deliverables address the needs expressed by the national / governmental CERTs in a satisfactory way.”
14.	To what extent do you agree with the following statement? “ENISA’s CERT related support and activities evolve in line with the needs and priorities of the CERT community.”
15. 16.	To what extent do you agree with the following statement? “ENISA has made a significant contribution in relation to the cooperation with and support to national and governmental CERTs (for instance, set-up of CERTs and cyber exercises).”
17.	To what extent do you agree with the following statement? “Sufficient means and channels are available to the CERT community in order to provide ENISA with feedback, suggestions and questions on its CERT related activities.”
18.	What additional CERT- related areas and activities would you recommend to ENISA, in line with the Cybersecurity Strategy of the EU, and/or beyond for coming 5 years?
19.	What is your opinion concerning the current strategic objectives of ENISA that are applicable to CERT area? Do they respond to the needs of your organisation? Are they sufficiently relevant?
20.	What ENISA communication channels are you the most familiar with? Which of them do you find the most useful with regards to the CERT specific activities? (For instance, website, quarterly review, reports, events, NIS brokerage, CERT Relations Mainlining list, other)
21.	Has your organisation ever made a request for ENISA support under the so-called Article 14?

QUESTIONS
22. If yes, how successful was ENISA in providing support in line with your expectations under Article 14?
23. Did you recently attend an ENISA CERT-related event (e.g. workshops, cyber exercises, trainings etc.)?
24. To what extent do you agree with the following statement? “The topics and presentations at ENISA’s CERT related events are relevant and useful to the CERT professionals.”
25. Did you recently attend an ENISA Cyber Europe exercise?
26. To what extent do you agree with the following statement? “ENISA Cyber Europe exercises and the related materials are relevant and useful to operational security professionals.”
27. To what extent do you agree with the following statement? “ENISA operational security reports and publications are relevant and useful.”
28. Would you recommend ENISA’s operational security reports and publications to others?
29. What additional CERT- focused areas and activities would you recommend to be covered during cyber exercises?
30. To what extent do you agree with the following statement? “Cyber Europe exercises help to develop practical cooperation between different stakeholders during cross-border incidents.”
31. To what extent do you agree with the following statement? “ENISA has contributed to enhancing national/governmental CERTs crisis management and cooperation capabilities”
32. To what extent do you agree with the following statement? “ENISA should take on a more active role in implementing the baseline capabilities, for example by doing on site assessment of CERTs and other operational communities to evaluate how the team is positioned in the community at large.”
33. Should ENISA define of what is a mature CERT or other operational security communities by for example working together with TF-CSIRT Trusted Introducer on a certification scheme or resulting in a “badge”?
34. To what extent do you agree with the following statement? “Based on its experience and expertise, ENISA is in a strong position to express clear recommendations in reports/ studies (as opposed to mere suggestions) to the overall CERT community.”
35. To what extent do you agree with the following statement? “ENISA should proactively endorse/support initiatives relevant to the CERTs and other operational security communities (for example AbuseHelper, etc.).”
36. To what extent do you agree with the following statement? “ENISA should develop practical materials such as a “playbook” on how to deal with incidents, and/or a “CERT toolkit” with advice on how to run a CERT, etc.”
37. To what extent do you agree with the following statement? “ENISA could support (through coaching and guidance) CERTs/operational security communities and LEAs on how to participate in Horizon 2020 calls to obtain additional funding (i.e. grants).”
38. To what extent do you agree with the following statement? “ENISA deliverables tackle the needs expressed by European operational security community and CERTs in a satisfactory way.”
39. To what extent do you agree with the following statement? “ENISA deliverables generally evolve in line with the needs and priorities at the level of the operational security community and CERTs serving constituency in the EU Member States.”
40. What is your perspective on ENISA’s role as a facilitator and/or sponsor in relation to CERT activities, and what direction do you think it should take for the next five (5) years?
41. In what areas related to operational security, should ENISA put more focus, in the coming period?
42. To what extent do you agree with the following statement? “ENISA CERT-related reports and publications are relevant and useful.”
43. Would you recommend ENISA’s CERT-related reports and publications to others?
44. To what extent have the ENISA cyber exercises, such as the Cyber Europe series, helped the Operational security community, including CERTs, to identify gaps and help towards stronger cooperation in Europe?
45. Are you aware of or do you monitor ENISA’s CERT activities, such as trainings, workshops and support for CERT set-up, etc.?
46. In what ways do ENISA activities apply to or do influence the activity of your CERT?
47. To what extent to you agree with the following statement? “ENISA CERT related reports and materials are relevant and useful.”

QUESTIONS
48. If yes, to what extent to you agree with the following statement? “ENISA CERT related events are relevant and useful for the activity of my organisation?”
49. Should ENISA take on a more active role in supporting the CERT community outside of the European Union?
50. Would you be interested in participating to large scale crisis exercises such as Cyber Europe?
51. How could you contribute to Cyber Europe exercises?
52. To what extent do you agree with the following statement? “In terms of active support to capacity building for CERTs, ENISA’s trainings to technical staff from EU institutions are relevant and useful.”
53. To what extent do you agree with the following statement? In terms of cooperation with European institutions, ENISA has achieved its objective to develop and enhance these relationships.
54. Which of ENISA communication channels do you find the most useful with regards to the CERT specific activities within the European institutions?
55. To what extent do you agree with the following statement? “ENISA is a good source of information for my CERT related activities/tasks.”
56. If yes, how successful was ENISA in providing support in line with your expectations under Article 14?
57. Did you recently attend an ENISA CERT-related training?
58. To what extent do you agree with the following statement? “The ENISA exercise materials are relevant and useful to CERTs and operational security professionals.”
59. To what extent do you agree with the following statement? “Cooperation between ENISA and EC3 should go beyond the current ENISA/EC3 workshops. Both organisations should be more involved at the level of operational cooperation.”
60. To what extent do you agree with the following statement? “ENISA should collaborate with the European Police College (CEPOL) to organise joint LEA/CERT trainings”.
61. To what extent do you agree with the following statement? “ENISA should develop operational procedures in support new activities introduced by the proposed NIS Directive.”
62. To what extent are ENISA CERT activities important in supporting the Cybersecurity Strategy of the European Union, in particular the goals related to co-ordination between NIS competent authorities, CERTs, law enforcement and defence?
63. To what extent do you agree with the following statement? “ENISA’s CERT related activities address in a satisfactory way the needs of my organisation – as they relate to CERT area.”
64. Which ENISA communication channels of them do you find the most useful with regards to the CERT specific activities?
65. To what extent do you agree with the following statement? “ENISA has contributed to enhancing national cybersecurity crisis management capabilities”
66. To what extent do you agree with the following statement? “ENISA should create a certified list of companies as trusted cybersecurity service providers”.
67. To what extent do you agree with the following statement? “ENISA is a primary source of information for my CERT related activities/tasks.”
68. In what ways do ENISA CERT activities apply to your organisation / business?
69. To what extent do you agree with the following statement? “ENISA should collaborate more with academia on supporting CERT developments.”
70. To what extent do you agree with the following statement? “ENISA should collaborate more with NIS or cybersecurity professional organisations on supporting the latest CERT developments.”
71. How are you using ENISA reports and material related to supporting the CERTs?
72. How are you involved in ENISA activities and events in the domain of supporting CERTs?

Annex B: Glossary

TERM	DESCRIPTION
CEPOL	European Police College
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CSIRT	Computer Security and Incident Response Team
EC3	European Cybercrime Centre
EC	European Commission
EDA	European Defence Agency
EEA	European Economic Area
EEAS	European External Action Service
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership for Resilience
EU	European Union
EU CSS	EU Cyber Security Strategy
EU-SOPs	European Standard Operating Procedures
FIRST	Forum of Incident Response and Security Team
H2020	Horizon 2020
ICS	Industrial Control Systems
ICT	Information and Communication Technology
JRC	Joint Research Centre
LEA	Law Enforcement Agency
MS	Member State
NIS	Network and Information Security
NLOs	National Liaison Officers
PGP	Pretty Good Privacy
PPP	Public-Private Partnerships
SOPs	Standard Operating Procedures
TF-CSIRT	CSIRT Task Force
TF-CSIRT/TI	TF-CSIRT Trusted Introducer
WS	Work Stream

Annex C: Bibliography

[1] ENISA, “Impact Assessment and Roadmap,” 2014.

[2] European Parliament and Council of the European Union, “REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004,” 21 May 2013. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN.

[3] ENISA, “Work Programme 2013,” 27 November 2012. [Online]. Available: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013.

[4] ENISA, “Work Programme 2014,” 29 November 2013. [Online]. Available: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014.

[5] European Commission, “COM(2010)245 final - A Digital Agenda for Europe,” 19 May 2010. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN.

[6] European Commission, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final,” 07 February 2013. [Online]. Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667.

[7] European Commission, “Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (NIS Directive) - COM(2013) 48 final,” 07 February 2013. [Online]. Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666.

[8] ENISA, “Baseline Capabilities of National / Governmental CERTs - Operational Aspects,” 2009.

[9] ENISA, “Good Practice Guide for Incident Management,” The European Network and Information Security Agency .

[10] ENISA, “ A Good Practice Collection for CERTs on the Directive on attacks against information systems,” the European Union Agency for Network and Information Security (ENISA), 2013.

[11] ENISA, “ENISA CERT workshops,” [Online]. Available: https://www.enisa.europa.eu/activities/cert/events/past-events.

[12] ENISA, “Train the trainers and multipliers workshop,” 09 2015. [Online]. Available: https://www.enisa.europa.eu/activities/cert/events/train-the-trainers-and-multipliers-workshop.

[13] “TRANSITS training,” The European Union Agency for Network and Information Security (ENISA), [Online]. Available: https://www.enisa.europa.eu/activities/cert/events/transits-training. [Accessed 2014].

[14] “Cyber Crisis Exercises,” ENISA, [Online]. Available: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce.

[15] TERENA, “TF-CSIRT,” [Online]. Available: www.terena.org/activities/tf-csirt/.

[16] FIRST, “Forum of Incident Response and Security Teams,” [Online]. Available: http://www.first.org/about.

[17] European Commission , “COMMUNICATION FROM THE COMMISSION on Critical Information Infrastructure Protection,” 2009.

[18] European Parliament , “Critical information infrastructure protection: towards global cyber-security,” June 2012. [Online]. Available: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167.

[19] E. Commission, “Digital Agenda for Europe,” 7 Feburary 2013. [Online]. Available: http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip.

[20] European Commission, “Digital Agenda for Europe,” 2013. [Online]. Available: http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip.

[21] ENISA, “Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS,” 04 12 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems.

[22] ENISA, “Standards and tools for exchange and processing of actionable information,” ENISA, 2014.

[23] ENISA, “Work Programme 2015 including Multi-Annual Planning,” 28 October 2014. [Online]. Available: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015.

[24] European Commission, "Connecting Europe Facility Cyber Security Digital Service Infrastructure," 2015. [Online]. Available: http://ec.europa.eu/digital-agenda/en/connecting-europe-facility#digital-service-infrastructures-dsis.

[25] Eurocontrol, "Eurocontrol," [Online]. Available: https://www.eurocontrol.int/.

[26] ENISA, " Clearinghouse for Incident Handling Tools," European Union Agency for Network and Information Security (ENISA), 2005-2014. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/chiht. [Accessed 2014].

[27] ENISA, "Detect, SHARE, Protect. Solutions for Improving Threat Data Exchange among CERTs," ENISA, 2013.

[28] ENISA new good practice guide for CERTs - Issuing alerts, warnings and announcements , "ENISA," The European Union Agency for Network and Information Security (ENISA, 2013. [Online]. Available: http://www.enisa.europa.eu/media/news-items/enisa-new-good-practice-guide-for-certs-issuing-alerts-warnings-and-announcements. [Accessed 2014].

[29] ENISA, "A flair for sharing - encouraging information exchange between CERTs," the European Union Agency for Network and Information Security (ENISA) , 2011.

[30] ENISA, "Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime," Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime , 2012.

[31] "2014 Honeynet Project Workshop," The European Union Agency for Network and Information Security (ENISA), 2014. [Online]. Available: https://www.enisa.europa.eu/activities/cert/events/honeynet-project-workshop. [Accessed 2014].

[32] "European FI-ISAC," [Online]. Available: http://www.cpni.nl/informatieknooppunt/internationaal/european-fi-isac.

[33] E. U. A. f. N. a. I. S. (ENISA), "CERTs by Country - Interactive Map," [Online]. Available: https://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map.

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

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number: TP-01-15-747-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-132-8
DOI: 10.2824/236326