Study on CSIRT landscape and IR capabilities in Europe 2025

V 1.0

FEBRUARY 2019

www.enisa.europa.eu

European Union Agency For Network and Information Security

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 EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists 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 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.

Contact

For queries in relation to this study, please use:

csirt-relations@enisa.europa.eu

PGP Key ID:	31E777EC 66B6052A
PGP Key Fingerprint:	AAE2 1577 19C4 B3BE EDF7 0669 31E7 77EC 66B6 052A

Legal notice
Notice must be taken that this publication represents the views and interpretations of ENISA, 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

Table of Contents

Executive Summary

This study details trends about the recent and current evolution of CSIRTs and Incident Response (IR) capabilities in Europe towards 2025 at a strategic and policy level. As stressed in the 2016 Directive concerning measures for a high common level of security of network and information systems across the Union[1] (NIS Directive), CSIRTs play a vital role in cyber resilience in a context of increasing dependency on digital infrastructures. They perform an important function throughout the crisis management process, from identifying security incidents, protecting organisations against attacks, disseminating information on threats and recovering from incidents. The analysis framework included the following aspects:

- Technology trends
- Legal and regulatory landscape
- Actors at the policy, strategic and operational levels
- Changing threat environment.

These trends and findings were identified by mapping new and less visible CSIRTs recently created and by investigating policies across Europe and their impact outside Europe. Eighty-one (81) new CSIRTs were identified and a corpus of 36 policy, regulatory, and strategic documents related to the development of cyber incident response capabilities were analysed. An overview of the findings of the raw data is presented in Chapter 4.

Finding 1 – The implementation of the NIS Directive fosters the adoption of a holistic approach towards IR and an upward alignment of national capabilities

The recent updates of some Member States' national cybersecurity strategies and of the transposition into national law of the NIS Directive show a harmonisation in terms of strategic objectives, structures and practices in the fields of IR and CSIRTs. With regard to international and European cooperation, the national cybersecurity agencies – an increasing number of them integrating the national/governmental CSIRT in their organization – tend to play a central role. With much of the detailed application of the NIS Directive left to the national implementing laws of Member States, there remains a risk of fragmentation in terms of capabilities. The role and scope of action of CSIRTs may indeed also vary from one country to the other.

Finding 2 - The NIS Directive may have a positive effect at the international level and provides the EU with a status of 'norm setter'

In Europe's neighbouring regions and to a lesser extent internationally, there is an emerging trend of harmonization of domestic legal frameworks with the EU legal framework in the field of cybersecurity. Together with the EU General Data Protection Regulation (GDPR)[2] implemented since May 2018, the impact of the NIS Directive outside the EU may illustrate the ability of the EU to reach political and normative consensus between nations on cybersecurity-related issues, and to act as a standard setter in areas such as data protection, privacy and transparency.

Finding 3 – IR capability development of national administration and operators of essential services emphasizes the relevance of collaboration at national and European level

[1] Directive (EU) 2016/1148 - http://data.europa.eu/eli/dir/2016/1148/oj

[2] Regulation (EU) 2016/679 - http://data.europa.eu/eli/reg/2016/679/2016-05-04

Operators of essential services in the seven sectors identified in the NIS Directive, as well as national administrations, accelerate their effort to build or upgrade their IRC. This effort includes the development of sector-specific CSIRTs and IR collaboration mechanisms and fora, both at EU and national levels. At a national level, the growing number of sector-specific and sector-wide CSIRTs could initiate a move towards the organisation of IR cooperation according to a vertical model, as a complement to the horizontal and centralized model built around the national government CSIRTs.

Finding 4 - Successful cooperation initiatives in the field of Incident Response Capabilities at an international level are driven by public-private partnerships

On the international stage, two main kinds of cooperation initiatives were identified in the field of IRC and cybersecurity at large: cooperation among global actors of the same sector, and the effort of the international community to address the international challenges of digital technology and security. These initiatives show a move toward more public-private partnerships in the field of cybersecurity is necessary at the international level, although security is a sovereign domain and states are reluctant to agree on binding measures. Addressing digital security indeed requires involving technology giants to define common norms in the governance of digital infrastructures and data.

Finding 5 – There is an important development of IR services in the European private sector; however, new vulnerabilities tend to target the hardware layer of devices manufactured outside Europe

In the longer term, the NIS Directive also has the objective to stimulate the competitiveness and innovation capacities of the digital industry in Europe by increasing the demand for cybersecurity and to support the development of a sustained supply of innovative cybersecurity products and services in Europe[3]. It seems that the NIS Directive and the overall recent increase in security requirements may have a positive effect on the European private sector by stimulating the supply of innovative cybersecurity services and products. However, supply chain attacks and the Meltdown and Spectre vulnerabilities suggest that new vulnerabilities and the corresponding threats are surfacing within the hardware layer. The difficulties associated with detecting and mitigating these types of vulnerabilities raises a question on the role and benefit of both national governmental CSIRTs and European cybersecurity services providers in the IR value chain, should vulnerabilities and cyber-attacks increasingly affect devices directly in the future.

Finding 6 – Acknowledging their exposure to cyber risks, military players tend to follow the same dynamics as the civilian sector when developing their IR capabilities

As demonstrated by the growing number of cyber defence commands in European armies, cybersecurity is now considered as an integral component of modern defence. It seems however that there are limited specificities for the military domain in the digital era: armed forces are undergoing a similar digitalisation trend as civilian actors, use similar tools, and therefore face similar security challenges. Taking into account the recognition that they may face the same threats as civilian actors, European armed forces are increasing and rationalise the organisation of their IR and offensive capabilities at a rather rapid pace, as witnessed by the establishment of new cyber units and components in European armies such as Czech Republic[4], Germany and France in 2017. In this endeavour, armed forces however must address additional challenges given the

[3] https://www.enisa.europa.eu/news/executive-news/discussion-on-implementing-the-nis-directive-and-enhancing-competitiveness

[4] In 2018, Czech Republic published a national cyber defense strategy to increase its capabilities during the 2018-2023 period: https://ccdcoe.org/cyber-security-strategy-documents.html

complexity and longer duration of their systems in a context of a fast-moving ICT (and cyber threat) landscape..

1. Overview and scope of the study

1.1 Context

In 2018, ENISA is concentrating its efforts on assisting Member States with their incident response capabilities by providing a state-of-the-art view of the CSIRT landscape and development in Europe. One of the main objectives of this work is to further develop and apply ENISA recommendations for the CSIRT capability development.

ENISA has a European CSIRT inventory on its public website[5], providing an overview of the current situation concerning CSIRT teams in Europe. This inventory provides a list of publicly listed incident response teams that can be visualised via an interactive mapping tool.

The CSIRT and Incident Response (IR) fields are fast changing by nature. The current drivers of these changes are for example:

- Creation of NSA-type and or Military CSIRTs;
- New types of sectoral CSIRTs are or must be created due to the NIS Directive;
- Organisations like the EU itself and NATO also have their own IR-CSIRT capabilities;
- In some EU member states, the National Cyber Security Centre has absorbed the National or Governmental CSIRT(s);
- The private sector and digital device manufacturers play an increasing role in incident response.

1.2 Objective of the study

The objective of this study is to help ENISA to identify and draw conclusions about the recent and current evolution of CSIRTs and IR capabilities in Europe towards 2025. Building on the existing knowledge gathered in the European CSIRT inventory, this study aims to dive deeper into the "blind spots" that may exist in this mapping.

The specific objectives of this study are:

- To do a mapping on an operational level of new and less visible CSIRTs created recently.
- To investigate on a strategic and policy level what is happening across Europe and outside the EU in order to reveal new structures that are emerging and to investigate the policies that drive these changes.
- To deliver insightful recommendations to ENISA capturing the key aspects of a state-of-the-art view of the CSIRT-IR landscape and development in Europe.

[5] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

1.3 Scope of the work and definitions

In addition to supporting the update of the ENISA European CSIRT Inventory, this study provides data and an analysis of the main developments in the field of Incident Response (IR) capabilities at strategic and policy levels.

The analysis focuses on providing insights on whether cooperation between the different players – in particular CSIRTs – is spontaneous or driven by regulation.

The prospective vision of the analysis tries to identify the key evolutions in the CSIRT-IRC landscape within a 5-year timeframe.

Computer security incident response team (CSIRT) landscape

"A CSIRT is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches"[6]. Other widely accepted terms exist for CSIRTs, such as CERT (Computer Emergency Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team) or SERT (Security Emergency Response Team).

This study extends the concept of CSIRT to cover formal entities performing this work, but not necessarily called CSIRT. The objective is to capture the latest trends in this field by also covering the most recent and emerging entities created which provide similar core services and coordinate the effort to respond to cyber threat.

The landscape focuses on entities operating on a large scale (countrywide capabilities, bigger players) and in strategic sectors. In this study, the concept of 'strategic sectors' covers:

- The seven sectors identified in the NIS Directive: healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply.
- Sectors directly related to national security and sovereignty: defence, justice and security.

The geographical focus of the CSIRT landscape is on the European Union (EU) Member States and the remaining European countries in Continental Europe (i.e. the Balkan region, the countries applying for EU membership).

Incident Response (IR) Capabilities

Incident response and management is the protection of an organisation's information by developing and implementing an incident response process (e.g. plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and then effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems[7].

[6] A step-by-step approach on how to set-up a CSIRT, ENISA, 2006.
[7] Strategies for Incident Response and Cyber Crisis Cooperation, ENISA, August 2016.

This study focuses on the current and future dynamics in the field of IR capabilities in Europe at a strategic and policy level. As with the CSIRT landscape, the research and analysis focus on strategic and sovereign sectors, and also includes international players such as NATO

The geographical focus in on the EU Member States and on the regions influencing or being influenced by the European Union legislation in this domain.

2. Methodology and data collection

2.1 Step 1 – Identification of CSIRT inventory's mapping of blind spots

The ENISA's inventory tool was used as the starting point to identify blind spots to avoid duplication of efforts when researching and analysing new entities. In addition to addressing the specific objectives of the study, the following blind sports were proposed and validated with ENISA at the beginning of the work:

- **Constituency type**: among the 344 CSIRTS identified, there was a majority of Commercial Sector, NREN, Governmental sector and Financial sector CSIRTs, while entities in Military organisations, CIP/CIIP sector, Law enforcement agencies, and non-commercial organisations were less represented;
- **Geographical coverage**: 15 Member States had less than 8 CSIRTs identified in the inventory.
    - All EU Members States have a national and/or government CSIRT
    - No EU Member State has CSIRTs for all critical sectors
    - 3 Member States have a CSIRT for the energy sector (Poland, Italy, and Austria)
    - 13 Member States have a CSIRT for the financial sector (Austria, Belgium, Czech Republic, Estonia, Germany, Italy, Luxembourg, Spain, and the UK)
    - 10 Member States have a CSIRT focusing on Critical Information Protection and / or Critical Information and Infrastructure protection (Belgium, Estonia, Germany, Italy, Luxembourg, Slovakia, Spain, and the UK)

2.2 Step 2 – Definition of data classification criteria

This step was dedicated to building an analysis grid to be used to classify the newly identified CSIRTs, by defining a set of analysis criteria.

The list of criteria was defined:

- Using the criteria of the ENISA CSIRT inventory: Country, CSIRT/Team name, Constituency, Contact.
- Adding additional criteria pertaining to the specific data sought in the context of this study (e.g. cooperation aspects, date of creation, etc.).

A list of criteria was also established for the collection of data pertaining to the IRC.

This step was conducted in close cooperation with the ENISA team to collect criteria that seemed important to them.

For detailed information on the selected criteria, see part 5.1 on Data classification and structuring.

2.3 Step 3 – Design of the data classification grid

During this step, the research team used the pre-defined classification criteria and the validated blind spots to build an analysis grid. The purpose of this analysis grid was to:

- To facilitate the data collection step by focusing the research work on the key topics of interest for ENISA;
- To present the raw data in a structured way.

2.4 Step 4 - Data collection

This step consisted in conducting a literature review to identify relevant resources to collect data on new CSIRTs and recent trends in the field of IRC. The research methodology was lean, efficient, and employed techniques to ensure an incremental data collection and research process.

The following resources were used:

- Policy documents;
- White papers and national security strategies;
- Publicly available reports from CSIRT's, National Cybersecurity Centres, Ministries and regional/international organisations;
- Operational and strategical Publications from research centres and academia;
- Publications from subject matter experts.

During a preliminary data collection phase, the relevant data were gathered in the data classification grid by a first team of analysts.

The preliminary data was then validated and further enriched by a second team of analysts.

2.5 Step 5 – Raw Data Analysis and trends evaluation

The methodology used in this step was based on a qualitative use of the **Delphi Method**[8]**,** which ensures that the data collection team and the data analysis team benefit from and build on each other's expertise, and that the final analysis addresses all aspects of the request presented in a concise, coherent and comprehensive way.

"The ***Delphi method*** *is a structured communication technique, originally developed as a systematic, interactive forecasting method which relies on a panel of analysts. The analysts answer questionnaires in at least two rounds. After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round. Thus, analysts are encouraged to revise their earlier answers in light of the replies of other members of the panel. It is believed that during this process, the range of the answers will decrease and the group will converge towards the "correct" answer. Finally, the process is stopped after a pre-defined stop criterion (e.g. number of rounds, achievement of consensus, and stability of results)."*[9]

Relying on the expertise of senior experts and analysts, the Delphi method was applied in a qualitative way to ensure that these different areas of expertise contributed to a comprehensive analysis. The objective was to:

- Validate that the full scope of study has been covered;

[8] https://www.rand.org/pubs/papers/P3558.html
[9] http://en.wikipedia.org/wiki/Delphi_method

- Validate the quality of the collected data;
- Discuss emerging trends for each specific domain (CSIRTs and IRC);
- Discuss the benefits of existing initiatives undertaken at the EU level in these domains;
- Identify additional information and topics that should be further explored.

Environment scanning techniques were also used to identify the strategic and operational trends that will affect CSIRT and IRC by 2025. Environmental scanning is conducted in order to:

- Broaden one's vision and perspective;
- Anticipate change;
- Understand emerging patterns and trends;
- Inform strategic perception, thought and anticipation.

A dedicated scanning framework was set up to guide the analysis. This framework included the following categories, such as:

- Nature of the threats;
- Technologies;
- Legislation and regulations;
- Policy actors.

These categories helped identify:

- The driving forces pushing or informing the main trends in the field of CSIRT/IR;
- Early signs or indicators to measure the CSIRT/IR developments;
- Potential impacts on the field of CSIRT/IR.

Once these analysis methods were applied, a first version of the key findings of the study was drafted and submitted to ENISA for validation and further discussion.

2.6 Final Reporting

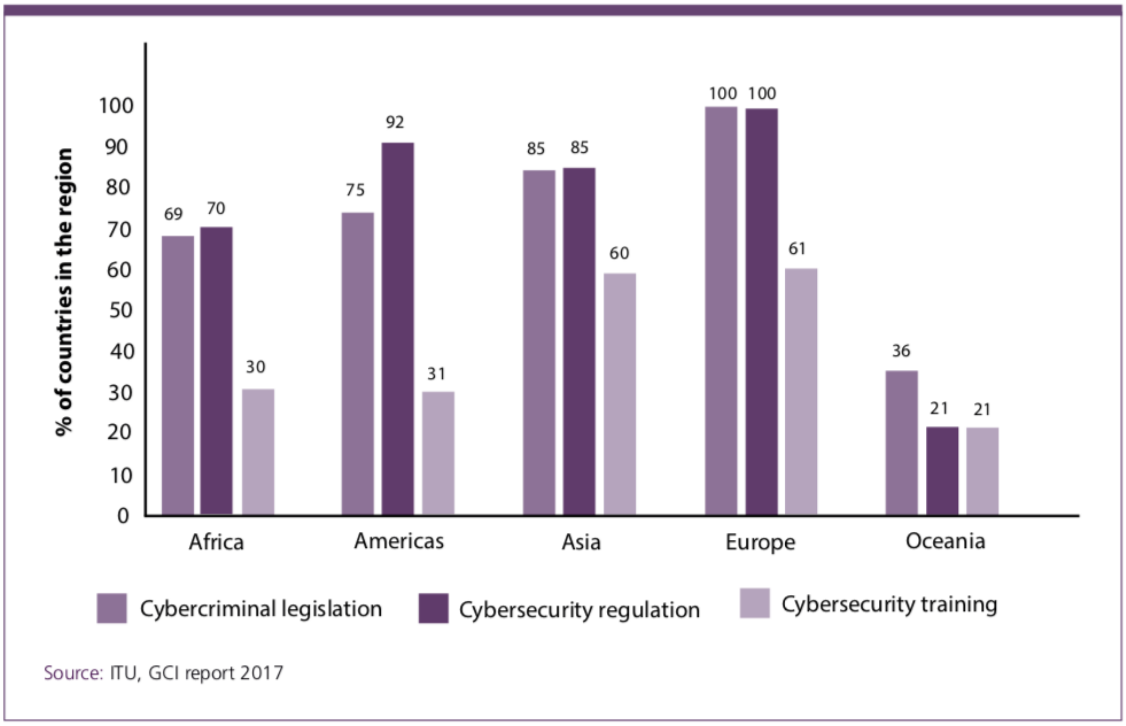
This final step consisted in further developing findings of specific interest to ENISA and in drafting the final report of the study.

Close interactions and exchanges with ENISA ensured that the final recommendations of the study were in line with the need and expectations of ENISA.

3. Key findings

3.1 Finding 1 – The implementation of the NIS Directive fosters the adoption of a holistic approach towards IR and an upward alignment of national capabilities

As highlighted in the recently published United Nations e-government survey 2018[10], all European countries have cybersecurity legislation and regulations in place.



Source: ITU, GCI report 2017

Figure 1 - Total number of Member States with laws related to cybercrime in 2017 (Source: UN)

The mapping and analysis of some of the recent updates of some Member States' national cybersecurity strategies and the NIS Directive's transposition into national law – some of them presented in the table below – show a harmonisation in terms of strategic objectives, structures and practices in the fields of IR and CSIRTs.

Concerning international and European cooperation, national cybersecurity agencies – an increasing number of them integrating the national and governmental CSIRTs into their organisation – tend to play a central role.

[10] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018

MEMBER STATES	IR AND CSIRT RELATED ASPECTS
Bulgaria: (Draft) Law on Cybersecurity[11]	Organisation, management and control of cybersecurity incident response; Designation of competent authorities in the field of cybersecurity, as well as their functions; Designation of competent authorities regulating the activities necessary measures to achieve a high level of network security and information systems.
Cyprus: Security of Networks and Information Systems Law	Creation of a National Digital Security Authority (NDSA); Inauguration of the Cyprus national CSIRT (CSIRT-CY) on 25 June 2018, which will be part of the NDSA; CSIRT-CY was established with the support of the ITU; CSIRT-CY is responsible for responding to incidents in all critical infrastructures in the Republic of Cyprus, such as the energy and water providers, ports, hospitals and financial institutions; Until 2018, there was no national computer-related incident response organisation with operational ability and the establishment of a national CSIRT was a long overdue CSIRT-CY has managed to secure EC CEF funding for further enhancements in 2019.
Estonia: Cyber Security Act	The national cybersecurity agency (RIA) is assigned the central role of organising cybersecurity at the state level; RIA is assigned the function of the cyber incident resolution unit; RIA fulfils the role of international point of contact, and is responsible for coordinating cross-border exchanges of information and IR measures taken at the EU level.
Italy: NIS Directive Implementing Decree	Identification of the NIS competent Authorities and their respective tasks; Replacement of the national CSIRT by merging the national CERT-N (Private sector) and the CERT-PA (Public Administration); Reinforcement of the cooperation both at national and at EU levels.
Netherlands: National Cyber Security Agenda (NCSA) 2018	The incident response capabilities of the intelligence and security services, Defence Computer Emergency Response Team (CERT), the National Cyber Security Centre (NCSC) and Rijkswaterstaat (Directorate-General for Public Works and Water Management) are being enhanced to be able to deal with ICT breaches that threaten national security;

[11] https://www.e-gov.bg/bg/212

	Situational awareness at the national level will be enhanced by the creation of a cooperation platform to offer more information and a swifter perspective for action with relevant organisations.
United Kingdom: NIS Regulations 2018	The National Cyber Security Centre (NCSC – part of GCHQ) acts as the UK's CSIRT and as the UK's single point of contact; NCSC remit is to provide support, expert advice and incident response assistance, and to develop cybersecurity guidance and standards, as well as holding an advisory role in relation to UK CSIRTs; In 2018, NCSC produced guidance and developed a framework, which supports the assessment of the level of cybersecurity achieved by OES in relation to NIS requirements.

These recent policy and regulatory orientations do not however indicate if this harmonisation of legislations will lead to an actual harmonisation and upgrade of the actual national IR capacities.

As illustrated in the table above, the implementation of the NIS Directive varies from one country to another, based on the experience of the country in the domain of cybersecurity and the degree of maturity of its national incident response capabilities, in particular CSIRT.

With much of the detailed application of the NIS Directive left to national implementing laws, there is a risk of fragmentation in terms of capabilities and of lack of visibility of the newly created national CSIRT and its actual capabilities. Their role and scope of action vary from one country to the other, and affect the cooperation with national law enforcement, judicial and military bodies.

As an example, the UK NCSC acts as the UK's CSIRT under the NIS regulation and will have a significant supporting and advisory role in providing IRC to cyber-attacks; however ultimate authority and responsibility for any regulatory decision with regard to cybersecurity in a specific sector lie solely with the competent sectoral authority.

Furthermore, since the NIS directive is a recent regulation, its full implementation will take time, and some countries still lack maturity and capacities in the field of IR.

At national level, there is also a strong trend of private-public partnerships, which seems to be a key success factor of IR. A recent example is the Belgian Cyber Security Coalition[12] set up in 2015, which brings together cybersecurity specialists from government organisations, companies and academia with a view to improving the protection of government organisations, the business world and private citizens against cybercrime in Belgium. To this end, the Coalition counts on the exchange of experiences between members as well as publications offering advice to companies and awareness campaigns aimed at the general public. The Coalition is also set to advise the government and the business world in drawing up guidelines on to cybersecurity.

[12] https://www.cybersecuritycoalition.be

3.2 Finding 2 – The NIS Directive may have a positive effect at the international level and provides the EU with a status of 'norm setter'

In Europe's neighbouring regions and to a lesser extent internationally, there is an emerging trend of harmonization of domestic legal directives and regulations with the ones created by the EU. As in the recent case of the EU General Data Protection Regulation (GDPR), the impact of the NIS Directive outside the EU may illustrate the ability of the EU:

- To develop political and normative consensus between countries on security-related issues;
- To act as a standard-setter in cybersecurity.

This leading role relates to areas such as data protection, privacy and transparency, e.g. by setting incident reporting obligations.

Some candidate countries for EU membership, in particular in the Balkans, have increased their cybersecurity legislation in recent years with specific references to the NIS Directive and relevant EU regulations.

Serbia, which was officially granted candidate country status for EU membership in 2012, provides an interesting illustrative case: in the process of developing its national information security regulatory framework – and more specifically in its Law on Information Security adopted in 2016[13][14] - Serbia takes into account existing EU legislation. Referring to European standards and directives, the Law introduced the National Centre for the Prevention of Security Risks in ICT Systems (National CERT), the CERT republic authorities, and the possibility of establishing special centres for the prevention of security risks in the ICT systems (Special CERT)[15].

Beyond candidate countries, Ukraine also provides a recent case of national cybersecurity regulations influenced by European standards. Its 2016 National Cybersecurity Strategy[16] acknowledges that "*the primary concerns of development of secure, stable and reliable cyberspace are to be as follows:*

- *Formation and operational adaptation of state cybersecurity policy on the cyberspace development, achieving compatibility with the relevant EU and NATO standards;*
- *Creating a national regulatory framework and term base in this area, harmonization of regulatory documents for electronic communications, information protection, information security and cybersecurity in accordance with international standards and standards of the EU and NATO*".

While highlighting the different approaches adopted by the United States (U.S.) and the EU in their endeavour to strengthen cyber-resilience, the reactions in the U.S. to the GDPR and the NIS Directive also suggest an increasing interest towards EU-led initiatives. The primary reason is that U.S. private companies doing business or with subsidiaries in the EU will have to update their cybersecurity practices and policies to ensure compliance with these new and expanding legal requirements. It is worth noting that lessons from NIS Directive compliance and from a more binding approach to cybersecurity will also be carefully assessed

[13] http://mtt.gov.rs/en/releases-and-announcements/two-laws-adopted-on-advertising-and-information-security/
[14] https://www.amcham.rs/upload/Zakon%20o%20informacionoj%20bezbednosti.pdf
[15] http://www.ubs-asb.com/Portals/0/Casopis/2017/4/UBS-Bankarstvo-4-2017-DarkoSehovic.pdf
[16] https://ccdcoe.org/sites/default/files/documents/NationalCyberSecurityStrategy_Ukraine.pdf

by U.S. stakeholders, while experts judge that '*the likelihood of the US government adopting similar legislation grows*'[17].

3.3 Finding 3 – IR capability developments of national administrations and operators of essential services emphasize the relevance of collaboration at national and European level

The above-mentioned (3.1) United Nations e-government survey 2018[18] identifies Europe as the region in the world with the highest presence of national, government and sectoral CSIRTs.

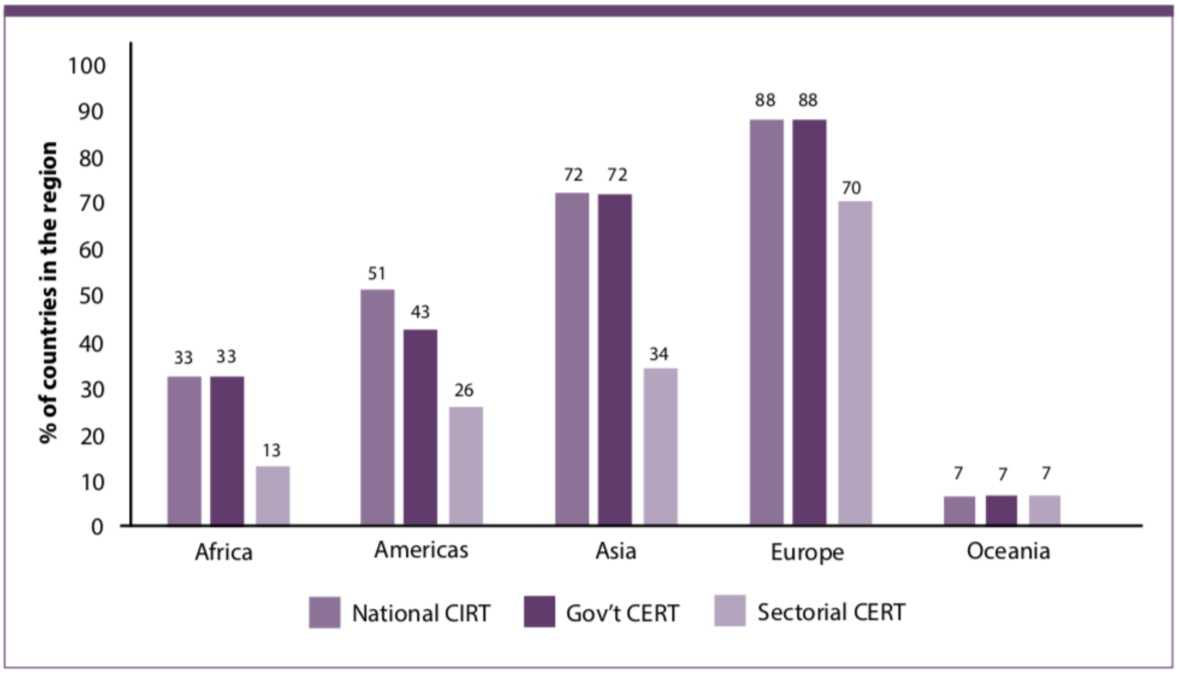


Figure 2 - Regional view of CERT/CIRT/CSIRT

In the EU, operators of essential services in the seven sectors identified in the NIS Directive as well as national administration are accelerating their efforts to build or upgrade their IRC. This effort includes the development of sector-specific IR collaboration mechanisms and fora, both at an EU and national level.

At national level, the trend towards sector-specific IRC may cause a reorganisation of IR cooperation towards a vertical model (rather than a horizontal and centralized model built around the national CSIRT).

Strengthening IR capability development of operators of essential services

The NIS Directive states "*Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations*"[19]. This requirement is in continuity –

[17] https://venturebeat.com/2018/07/07/while-everyone-was-focused-on-gdpr-the-nis-directive-snuck-in-through-the-back-door/?ref=techi.com
[18] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018
[19] Chapter IV, Article 14 - https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

and is an additional catalyst – of a strong trend in which operators of essential services set up a CSIRT within their organisation.

The table below presents a few examples of recent teams created in recent months.

SECTOR	NAME ORGANISATION & CSIRT	DATE OF CREATION
Transport	Deutsche Bahn - DB Systel CSIRT	2017
Banking & Finance	Dutch Association of Insurers - iCERT	June 2017
	Nordic Financial CERT - NfCERT	2017
	Finish Tax administration - Nixu Cyber Defence Centre	September 2017
Health	PGGM (Pension Fund) - PGGM-CERT	March 2017
	Sykehuspartner CERT	2017
	Z-CERT	Operational since June 2017
Energy	EDF Group – CERT EDF	Currently being established
Digital infrastructure (and telecommunications)	Engie Group – CERT Engie	2018
	Norwegian Communications Authority (NKOM) – EkomCERT	July 2017
National administrations	Norwegian Government Security and Service Organisation – DSS CERT	October 2016
	Agency for technological modernization of Galicia – CSIRT.gal	February 2018
	Czech Republic Local Administration – KBM-CSIRT	April 2016
	Hessian Sate Administration - CERT-HESSEN	2017
	Federal Office for Information Security (BSI) - MIRT - Mobile Incident Response Team	2017
	CCN-CERT – Foro CSIRT.es	2018

Capacity building may also extend to smaller market players following a more horizontal approach. For example, a German company created a CERT called CERT@VDE[20], specifically dedicated to small and medium-sized enterprises (SME) and with a focus on Industrial IoT and Industry 4.0.

There are, however, different levels of maturity in the IRC domain from one sector to another. On the one hand, highly digitalized sectors such as banking and finance appear very mature, in particular when it comes international and European cooperation. On the other hand, more traditional industrial sectors such as transport and energy rely on heavy industrial systems, which are more vulnerable because they have not been designed to deal with malicious acts. This is also due to the fact that the lifetime of their operational facilities is often very long (more than 10 or 15 years) and need to adapt to the extremely short cycles of Information Technology, lest they accumulate vulnerabilities due to the obsolescence of their IT layer.

An example of these capability gaps is given by a 2017 report published by the Vlaams Nederlandse Delta (VNDELTA), pointing out that "*few organisations have dedicated IT security staff and none have a mature security incident detection and response team*" in the ports of the Belgo-Dutch provinces, including major ports such as Rotterdam[21].

Initiating collaboration at national, regional and a European level

Acknowledging the growing interdependencies between their infrastructures and services, existing and recently established CSIRTs of operators of essential services place collaboration at national, a regional and European level among their key strategic objectives.

At national level, sharing information and reports with other CSIRTs, facilitating contact with appropriate law enforcement agencies, and participating in national emergency and crisis exercises are the common objectives of all CSIRTs. At sector level, CSIRTs provide awareness raising and information sharing services rather than incident response capabilities, with several ISACs (Information Sharing and Analysis Centres) already in place.

However, as illustrated in the two examples presented below, there is an emerging trend, which sees actors, and CSIRTs in the same sector go beyond information sharing to organise and pool IR capabilities.

In this regard, one should consider the cases of Member States (such as France), who already established some sector-specific cooperation schemes that may further lead to a vertical organisation of IRC. While national governmental CERTs have traditionally played a central role in coordinating information exchange, incident response, and capacity building in the different sectors of the economy, the increasing needs and numbers of actors impose a more vertical organisation for each sector. The challenge in this context is to avoid organisational silos as well as excessive disparities among actors.

National level

A pioneering initiative in this regard is the Austrian Energy CERT[22], which became operational in 2017. It may provide a positive role model for establishing cooperation mechanisms in the energy sector at the EU level.

The creation of this CERT is one of the main outcomes of a public-private partnership launched in 2013 by different players of the energy domain in Austria, with the objective of improving understanding and

[20] https://cert.vde.com/de-de
[21] http://www.vndelta.eu/files/3215/1125/0649/Cyber_Security_in_Ports_Whitepaper_VND_vonference_november_2017.pdf
[22] https://www.energy-cert.at/de/

addressing common security risks and interdependencies[23]. Twenty companies are currently directly involved in CERT Energy and two national professional associations, which played an important role in the setting up the CERT, represent other smaller players. The basic services of the CERT have been fully operational for one year and include:

- Establishing situation reports and alerting members in case of crisis,
- Supporting the incident management of one of the members with centralised IRC,
- Improving the capacities of the members through common exercises and training,
- Establishing security concepts, and increasing risk awareness at multiple levels, in particular for top management.

The experience of the Austrian Energy CERT has shown that the main benefit of pooling and sharing IRC is enabling information sharing and collaboration among trusted actors. Beyond the national scene and in the context of the NIS Directive, the Energy CERT will also facilitate the choice of a common point of contact for the Austrian energy sector. It also facilitates collaboration with other Member States and international organisations in the energy sector. It is however worth noting that it took about 4 years to establish the consortium, set the common rules and agree on contractual terms.

Regional and European level

At regional level, the Nordic Financial CERT (NfCERT), founded in Oslo in June 2017, aims to strengthen the Nordic financial industry's resilience to cyber-attacks, by enabling Nordic financial institutions to respond rapidly and efficiently to cybersecurity threats and online crime[24]. The rationale underlying the creation of the NfCERT is that criminals do not care about borders and, therefore, there is a need to establish information exchange about what is going on in the neighbouring countries and learn from each other.

IR capacity building actions at a regional level are also implemented by the International Telecommunication Union (ITU), which is the United Nations specialized agency for information and communication technologies (ICTs). As such, ITU carries out a variety of actions and activities to build and strengthen incident response capacities at national and regional levels. The Buenos Aires Action Plan for Europe for 2018-2021 outlines the regional initiatives the ITU[25]. The fourth initiative, « Enhancing trust and confidence in the use of information and communication technologies », focuses on supporting the deployment of resilient infrastructure and secure services in Europe through:

- The elaboration or review of national cybersecurity strategies
- The setting up or improvement of the capacities of national CSIRTs and the building up of a network between these structures
- The organisation of simulation exercises at national and regional level

From 2013 to 2015, ITU assisted the Cyprus government to establish a national CSIRT[26] (see p.11). The ITU also conducts what is describes itself as a 'CIRT capability assessment'. Again, according to ITU on its

[23] This information is taken from a presentation given at the 'Cybersecurity in the Energy Sector #CySecEn High-level conference' on 11 October 2018 by the European Commission and the Austrian Presidency - https://ec.europa.eu/info/sites/info/files/programme_-_high_level_conference_cybersecurity.pdf
[24] https://www.nfcert.org
[25] https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/Brochure%20Regional_Initiaitves_EUROPE-E.pdf
[26] https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9CYP13001

website[27] the aim of this is 'to define the readiness to implement a national CIRT'. However, there is no detailed information available on what this means and no mapping or comparison is possible with other assessments like the one provided by ENISA[28]. In Europe and Commonwealth of Independent States (CIS), 8 countries, mostly in Eastern Europe, have been evaluated: Albania, Armenia, Bosnia and Herzegovina, Cyprus, Macedonia, Monaco, Montenegro, Serbia. Within the ITU, the Telecommunication Development Bureau (BDT) organizes ITU ALERT (Applied Learning for Emergency Response Teams), a capacity building exercise targeted at national CSIRTs, public institutions, telecommunication operators and the academia. ITU ALERT for Europe Region will be held from 26-30 November in Cyprus[29].

3.4 Finding 4 – Successful cooperation initiatives in the field of IRC at an international level are driven by public-private partnerships

On the international stage, two main kind of initiatives were identified pertaining to cooperation in the field of IRC and cybersecurity to a larger extent: cooperation between global economic actors of the same sector, and digital diplomacy.

What these initiatives have in common is that they illustrate:

- More public-private partnerships in the field of cybersecurity are necessary at the international level, although security is a sovereign domain;
- Addressing digital security indeed requires involving technology giants owning the digital infrastructures and data;
- Sovereign states show an unwillingness to agree on binding measures to regulate their behaviours and favour a voluntary approach.

1) **There have been a number of international cooperation initiatives between global actors of a specific critical sector**. In March 2018, a group of financial services experts, convened by the World Economic Forum, proposed 19 solutions for systemic cybersecurity threats in the financial sector. The objective is to provide a toolkit to identify cyber-risk management improvements in an innovative and fast-changing environment through public-private partnerships as well as concrete examples of how the framework can be applied in practice[30]. This is another example of the leading role played by the financial sector, whose players increasingly link technology companies to their system infrastructure – either voluntarily or because of regulation such as the European Union's Payment Services Directive 2 – making it crucial to have reliable cybersecurity.

2) **On a diplomatic and geopolitical level,** a proposal to regulate state behaviours in cyberspace has long been discussed in the framework of the United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, to address tangible gaps in the existing legal framework. This work has however achieved limited results, mainly due to the non-binding nature of these norms and the reluctance of some countries to regulate their own governmental activities in cyberspace. Interestingly the non-binding

[27] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx
[28] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey
[29] https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBDRILL/ITU-ALERT-Cyber-drill.aspx
[30] http://www3.weforum.org/docs/WEF_Cyber_Risk_to_Customer_Data.pdf

norms drafted by the states are similar to the principles initially proposed by Microsoft. It indeed appears that while the achievements of the UNGGE are limited, numerous initiatives have been launched in recent years by states, companies and international organisations: the Microsoft Tech Accord[31] and call for a Digital Geneva Convention, the Siemens "Charter of Trust"[32], and the work of the Global Commission on the Stability of Cyberspace[33] (GCSC). These initiatives highlight the importance of bringing together public and private actors to tackle the challenge of security on the international stage. On the 12th November 2018 at the UNESCO Internet Governance Forum (IGF), President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace[34]. This high-level declaration on developing common principles for securing cyberspace has received the backing of States, as well as private companies and civil society organizations.

[31] https://cybertechaccord.org

[32] https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html

[33] https://cyberstability.org/about/

[34] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

3.5 Finding 5 – There is an important development of IR services in the European private sector, however new vulnerabilities tend to target the hardware layer of devices manufactured outside Europe

On the longer term, the NIS Directive also aims to stimulate the competitiveness and innovation capacities of the digital industry in Europe by increasing the demand for cybersecurity and to support the development of a sustained supply of innovative cybersecurity products and services in Europe[35].

In this regard, the mapping of recently created CSIRTs tends to show that the development of IR capability – in particular for operators of essential sectors - also relies on managed detection and response (MDR) services provided by commercial organisations. This offer aims to remove the burden of having to figure out 'what method or device to use' for an incident monitoring and response capability. MDR services includes security monitoring and alerting, and remote incident management. According to Gartner, the global MDR market came to approximately 100 million dollars in 2017 (a 15% increase compared to 2016).

In the ENISA European CSIRT inventory, commercial organisations are the most represented constituency. It seems therefore that the NIS Directive and the overall recent increase in requirements may have a positive effect on the European private sector by stimulating the supply of innovative cybersecurity services and products.

Another interesting trend is to be considered. The concept of 'cybersecurity-by-design' is being widely promoted, but its implementation is still below the expected considering the growing number of vulnerabilities found a patched by digital devices providers and hardware manufacturers every year. As pointed out in this ENISA info note[36], the number of disclosed vulnerabilities each year keeps on growing at a high rate. As also stated in the same info note, there are now also important vulnerabilities identified within the hardware layer. The Meltdown and Spectre vulnerabilities revealed in early 2018 illustrate this trend: Meltdown and Spectre exploit critical vulnerabilities in modern processors[37]. These hardware vulnerabilities allow programmes to steal data, which is being processed on the computer. Even though there are still fare more vulnerabilities being identified in the software layer, the ones like Meltdown and Spectre that target the hardware layer are much harder to mitigate, as clearly stated in this[38] ENISA info note: 'In the realm of the security vs performance discussion, whatever the opinion is, ultimately confirms that microprocessor manufacturers need to identify new ways to address these issues or vulnerabilities will continue to occur: manufacturers will continue to announce improved performances, and be forced to patch those after release'. In 2016, ENISA published a Hardware Threat Landscape and Good Practice Guide on this topic[39].

Other types of attacks targeting the hardware layer are the so-called 'Supply Chain Attacks'[40] and attacks directed at Industrial Control Systems (ICS)[41],

[35] https://www.enisa.europa.eu/news/executive-news/discussion-on-implementing-the-nis-directive-and-enhancing-competitiveness
[36] https://www.enisa.europa.eu/publications/info-notes/is-software-more-vulnerable-today
[37] https://www.enisa.europa.eu/publications/info-notes/meltdown-and-spectre-critical-processor-vulnerabilities
[38] https://www.enisa.europa.eu/publications/info-notes/security-vs-performance-discussion-with-the-return-of-201cspectrum201d-vulnerability
[39] https://www.enisa.europa.eu/publications/hardware-threat-landscape
[40] https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks-back-on-the-agenda
[41] https://www.enisa.europa.eu/publications/maturity-levels

In this context, device manufacturers develop their own CSIRTs, sometimes called PSIRT (Product Security Incident Response Team): IBM, Cisco, Huawei etc. This offer will most likely expand, as the IoT is constantly expanding, touching the daily lives of most citizens through smartphones, smart devices and the digitalization of everyday objects. Recently, a group of vendors proposed a cyber-risk management turnkey solution: Apple, Cisco, Allianz and Aon launched an integrated solution to manage risks associated with ransomware and other malware, which includes software and communication technologies, devices, and insurance coverage[42].

These trends raise a question pertaining to the benefit of both national/governmental CSIRTs and European cybersecurity services providers in the IR value chain, and their ability to play a central role should vulnerabilities and cyber-attacks directly affect devices.

It would therefore be interesting to further study the impact of the NIS Directive on the European cybersecurity industry, to further analyse if the growing demand (from regulators) for security is met by European actors or by foreign companies, primarily the United States and other regions where the main manufacturers of hardware are located.

3.6 Finding 6 – Military players tend to follow the same dynamics as the civilian sector when developing their IR capabilities

IR capacity building in European armed forces

As demonstrated by the growing number of cyber defence commands in European armies, cybersecurity is now considered as an integral component of modern defence. While the nature and the constrained environment in which armed forces operate impose a higher level of resilience, forces are going through a digitalization trend similar to that observed in the world because they are using similar tools, and are therefore facing similar security issues.

This situation is even more interesting since armed forces have long thought they were untouchable to a certain degree as they use specific and isolated networks, procedures and tools.

This changing situation can be illustrated by the following examples:

- In 2009, the Conficker computer worm infected the French Navy computer network.
- The newest Royal Navy aircraft carrier is equipped with the 2001 Windows XP OS, which was ‘state-of-the-art’ when the HMS programme was launched[43]. This OS was targeted by the WannaCry ransomware attack in May 2017 that disrupted public administrations and companies worldwide. According to a report by The Guardian newspaper, some Windows XP incidents were spotted on the ship's computers.
- In September 2018, the U.S. Senate released a report demonstrating to what extent the U.S. armed forces struggled and often failed to incorporate cybersecurity into key aspects of their processes and systems and stating how easy it was for cybersecurity test teams to compromise these systems[44].

[42] https://www.csoonline.com/article/3254527/security/apple-cisco-aon-and-allianz-partner-in-cyber-risk-management.html

[43] https://www.theguardian.com/technology/2017/jun/27/hms-queen-elizabeth-royal-navy-vulnerable-cyber-attack.

[44] https://www.gao.gov/assets/700/694913.pdf

There is therefore a structural difficulty for armed forces to ensure the cybersecurity of their digitalized systems, given the complexity of these systems and their lifecycle in a context of a fast-moving ICT (and cyber threat) landscape.

Recognising that they may face the same threats as civilian actors, European armed forces are increasing their IR and offensive capabilities of at a rather rapid pace.

As an example, the German government agreed on 29 august 2018 to create a Federal Agency for Innovation in Cyber defence[45] to develop cutting-edge defence technology and state-of-the-art offensive capabilities. In the Czech Republic, the creation of a National Cyber Forces Centre[46] (NCFC) was initiated in 2016 and this new capacity should be operational in 2020.

In France, a Cyber Defence Command[47] (COMCYBER), placed under the authority of the Chief of the Defence Staff, gathers as of 1 January 2017 all cyber defence forces of the French armed forces under the same operational, permanent and joint authority.

While there is little information available in open source on these recently created or strengthened military capabilities, it also creates a significant demand for IT experts and specialists that armed force are struggling to address.

IR cooperation at international and European level

Military cooperation in the field of cybersecurity takes place in the framework of both NATO and the European Union.

1) **NATO**-own IR capabilities are limited and depend on Allies' capabilities, except the NATO Computer Incident Response Capability (NCIRC), which is the IR team for NATO infrastructure itself. As such, NATO action focuses more on operational cooperation and interoperability between Allies' capacities during operations.

   At its Brussels Summit in 2018, Allies agreed to set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure, to be fully operational in 2023. When fully operational, the centre aims to coordinate NATO's cyber deterrent through a 70-strong team of experts. However, it is still uncertain whether this would lead to providing NATO with its own capability or only integrating Allies' national cyber capabilities into NATO missions[48].

   The approach towards cybersecurity promoted by NATO is that standards are increasingly decided by the industrial actors, and decreasingly by states, as evidenced by the decision to downscale its standardisation body from an agency (NSA) to a mere office (NSO) in 2014. As highlighted in a recent report by the European Parliament, NATO recognizes that "*Technological innovations and expertise from the private sector are crucial to enable Allied countries to mount an effective cyber-defence. Industry is the main supplier of hardware and software used by the military staff, also for operations".* This led NATO to launch the Industry Cyber Partnership in 2014.

[45] https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/08/cyberagentur.html

[46] https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf

[47] http://discours.vie-publique.fr/notices/163003632.html

[48] http://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-why-nato-s-cyber-operations-center-is-a-big-deal and https://www.cfr.org/blog/what-did-2018-nato-summit-accomplish-respect-cyber-issues

2) **At the EU level,** two of the 17 projects approved in the framework of the Permanent Structured Cooperation (PESCO) tackle cyber defence and IRC:

   a. The first, led by Lithuania, aims to establish an **EU Cyber Rapid Response Force**. So far, 7 countries have signed the Declaration of intent[49].

   b. The second, led by Greece, aims to create a **Cyber Threats and Incident Response Information Sharing Platform**.

   However, these initiatives are recent and limited information is available to evaluate operational cooperation at the European level in the field of IRC and its tangible impact. While highlighting the current political will to lay the foundation for joint and stronger European cyber defence capabilities, their implementation will measure the ability to build common capabilities and a common capacity to act beyond joint training.

[49] https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en

4. Presentation of the findings in the raw data

4.1 Data structuring and classification criteria

4.1.1 CSIRT landscape

The raw data gathered during the study was consolidated in an excel table. It was first classified based on the following sectoral and geographical criteria:

- Critical infrastructure (EU + EFTA countries)
  - Transport
  - Banking
  - Health
  - Financial Market Infrastructure
  - Energy
  - Drinking water supplies
  - Digital infrastructure (and telecommunications)
  - Cross-sectors
- Military and law enforcement (EU + EFTA)
- Government and Public administrations (EU 28 + EFTA)
- Other European countries
- NATO (as an organisation)
- European Union (as an organisation)

Then, for each CSIRT identified, the following information was provided, when available:

- Name of the entity
- Parent organization (home organisation of the entity)
- Date of creation
- Constituency (based on ENISA inventory)
- Country
- CSIRT-related activities and role
- Website/link (website of the entity, if it has its own)
- Cooperation aspects
- References (sources of the information gathered)

4.1.2 IRC landscape

The raw data gathered during the study was consolidated in an excel table. It was first classified based on a geographical criterion:

- EU 28 + EFTA
- Other European countries
- NATO (as an organisation)
- European Union (as an organisation)
- International

Then, for each IRC initiative identified, the following information was provided, when available:

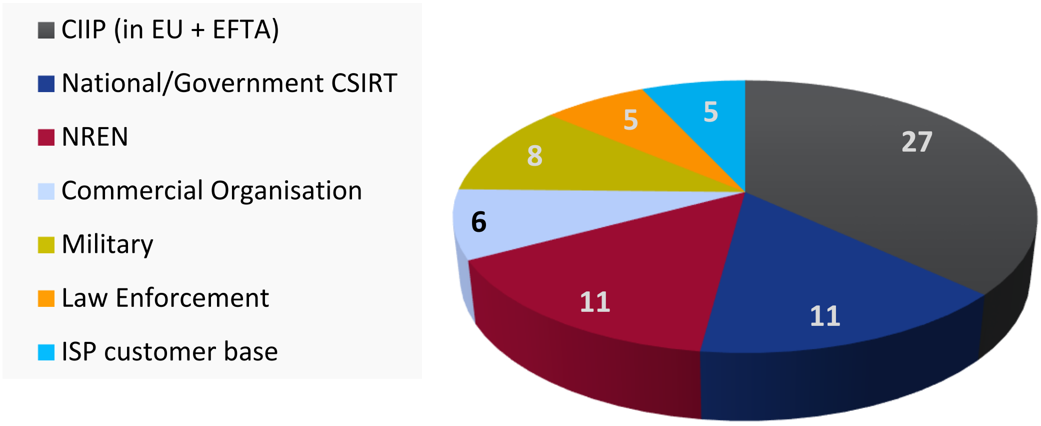
- Name
- Nature (legislation, strategy, activity report/study or stakeholder group/organization)
- Origin/source (authority/organisation at the origin of the initiative)
- Date of publication/creation
- Country/Region
- Key IRC-related aspects
- Cooperation aspects
- Comment
- References (sources of the information gathered)

4.2 Overview of the CSIRT landscape

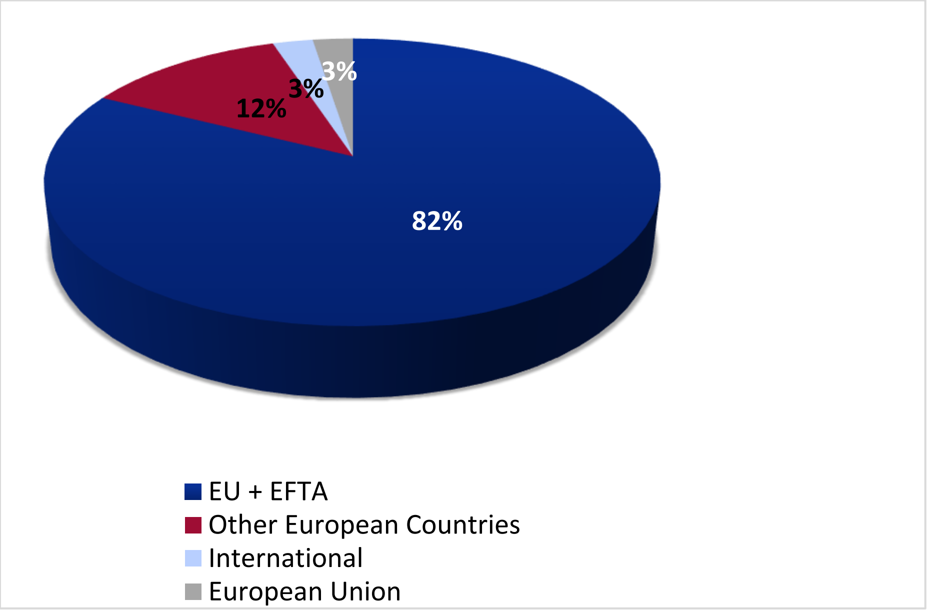
NEW CSIRT IDENTIFIED	ENISA INVENTORY	NEW DATA COLLECTED[50]	TOTAL
*Total CSIRT in the Inventory**	*363*	*81*	*444*
CIIP (EU + EFTA)	22	27	49
EU + EFTA	314	66	380
Other European Countries	30	10	40
National/Government CSIRT	97	11	108
Military	16	8	24
Law Enforcement	6	5	11
International	17	2	19
European Union	1	2	3
NATO	1	0	1

[50] Some of the CSIRT may fall into several categories (e.g. CIIP and International)

4.2.1 Identified CSIRTs by constituency

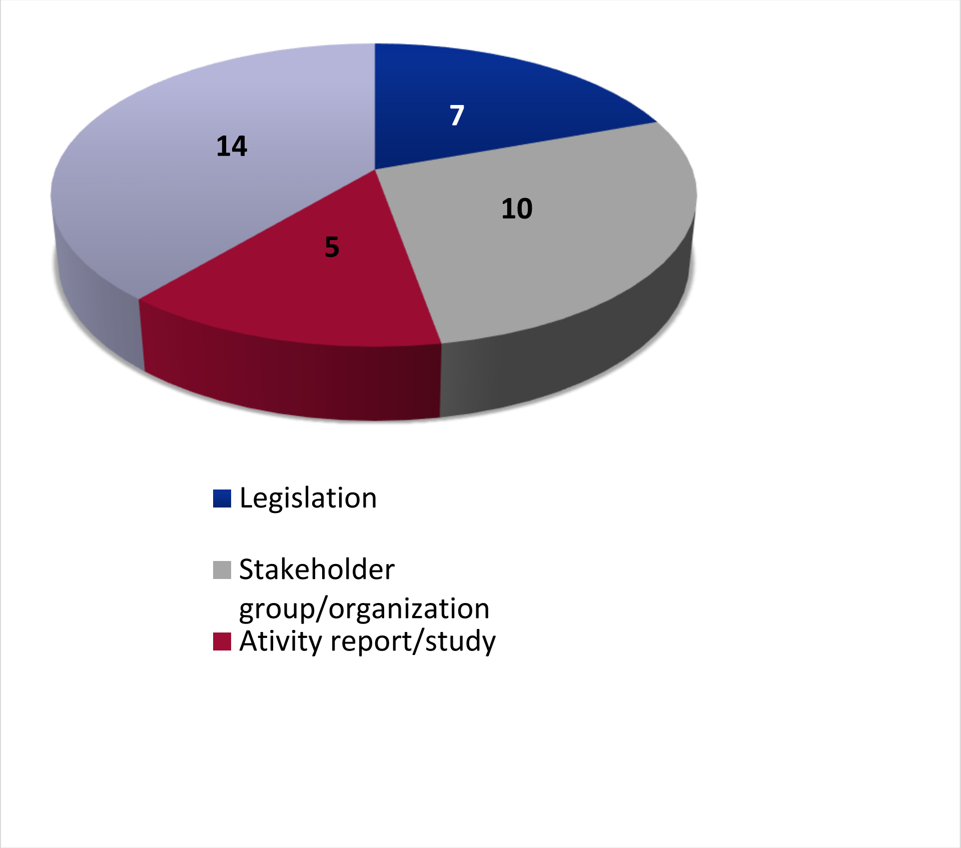


4.2.2 Identified CSIRTs by region



4.3 Overview of the IRC data

4.3.1 Analysed IRC by type of documents



5. Conclusion

This study has sought to collect data about and identify recent and current evolution of CSIRTs and Incident Response (IR) capabilities in Europe towards 2025 at a strategic and policy level.

Mapping on an operational level of new and less visible CSIRTs created recently

These trends and findings were identified by mapping new and less visible CSIRTs recently created, and eighty-one (81) CSIRTs were identified and analysed.

The collected data shows an increasing number of sectoral CSIRTs being created in the EU by public and private organisation operating essential services. In this regard, the important number of cybersecurity regulations in the EU appears as a key factor of this important cybersecurity capacity effort.

There are, however, different levels of maturity in the IRC domain from one sector to another. On the one hand, highly digitalized sectors such as banking and finance appears very mature, in particular when it comes to international and European cooperation. On the other hand, more traditional industrial sectors such as transport and energy rely on heavy physical infrastructures, which are more vulnerable because they have not been built with cyber security features by design and imply important investments to be protected.

The mapping and analysis of recent updates of some Member States’ national cybersecurity strategies and the NIS Directive's transposition into national law also show a harmonisation in terms of strategic objectives, structures and practices in the fields of IR and CSIRTs.

With much of the detailed application of the NIS Directive left to national implementing laws, there is however still a risk of fragmentation in terms of actual capabilities.

Emerging structures and trends at a strategic and policy level, and the policies driving these changes.

On a strategic and policy level, the analysis of a corpus of 36 strategic and regulatory documents enabled the analysis of what is happening across and outside the EU in order, in particular with the NIS Directive

This analysis shows that existing and recently established CSIRTs, in particular for those of operators of essential services, place collaboration at national, a regional and European level among their key strategic objectives.

The data also shows and recalls that cybersecurity is – to a large extent – driven by regulations[51]. In this regard, the NIS Directive and the GDPR play a key role in constraining actors to upscale their cybersecurity capabilities and standards, as well as increase their cooperation with other players.

At an international level, the lack of harmonised means and practices among countries in the cyberspace is mainly due to the absence of binding norms regulating their activities. The current effort made by the UN to agree on common regulations also supports the assumption that without the legal constraint, actors may be less willing to cooperate in the field of cybersecurity.

[51] See for instance the 2017 CXP Group analysis of cybersecurity key trends for 2017: https://www.pac-online.com/download/26609/187191

In Europe, the identified successful bottom-up driven collaboration – be it a national (Austrian Energy CERT) or regional (Nordic Financial CERT - NfCERT) - however shows the increasing awareness of market players of their interdependencies due to their digitalized infrastructures and services. These examples remind that there has been for many years voluntary information sharing among CSIRT community in Europe.

ENISA
European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki,
Greece Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu