Building a Cybersecurity Digital Service Infrastructure (DSI) and increasing national cybersecurity capabilities

How cybersecurity is funded in the European Union

Stéphane Hurtaud
Partner
Information Technology Risk,
Cyber Risk Services Leader
Deloitte Luxembourg

Petra Hazenberg
Partner
Lead Client Service Partner
European Institutions
Deloitte Luxembourg

Gunnar Mortier
Senior Manager
Information & Technology Risk
Deloitte Luxembourg

Alexander Cespedes Arkush
Manager
Information & Technology Risk
Deloitte Luxembourg

What is Cybersecurity in the EU about?

Cybersecurity refers to the safeguards and activities to protect cyberspace from threats that may harm its interdependent networks and information infrastructure, to preserve the availability and integrity of the networks and infrastructure, as well as the confidentiality and availability of its information. This is a challenge shared by all Member States of the European Union (EU).

The need for enhanced cybersecurity cooperation

A cooperation mechanism between cybersecurity stakeholders is essential to enable them to provide adequate levels of cybersecurity in the EU. Various actors have differing roles in cybersecurity cooperation. Such actors include the European Commission, regulators, industry and national and governmental (n/g) Computer Security Incident Response Teams (CSIRTs).

Amongst them, n/g CSIRTs are playing a key role in enhancing the cooperation by addressing cybersecurity incidents on a Member State and EU level.

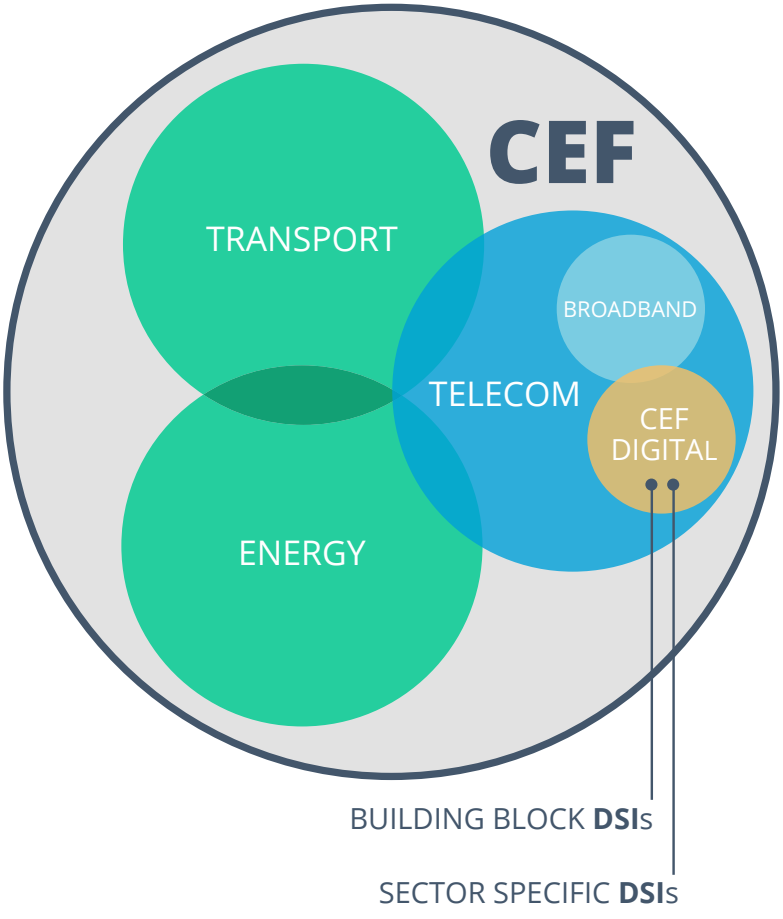
However, many CSIRTs lack resources, have insufficient supporting infrastructure and tools, have differences in maturity levels and are confronted with the challenges of sharing information that is potentially confidential and/or personal. As a result, the potential EU-wide cooperation has not reached its fullest potential yet. Cybersecurity stakeholders indicate that funding of national and EU-wide capabilities would be one of the key challenges to be addressed.

What is Connecting Europe Facilities (CEF)?

The Connecting Europe Facility[1] (CEF) is an EU funding mechanism to support the development of interconnected trans-European networks in the fields of transport, energy and telecommunications.

Between 2014 and 2020, CEF contributes to the goals set for the European single market by making 33,24 billion euro available in the form of funding for projects, various grants and other innovative financial instruments.

CEF investments are aimed at addressing the missing connections in Europe's energy, transport and telecom (including digital networks) through the deployment of Digital Service Infrastructures (DSIs). DSIs are defined in the CEF Telecom Guidelines as infrastructures which enable networked services to be delivered electronically, typically over the Internet, providing trans-European interoperable services of common interest for citizens, businesses and/or public authorities, and which are composed of Core Service Platforms and Generic Services.



1 https://ec.europa.eu/digital-single-market/en/connecting-europe-facility

What are Core Service Platforms?

Core Service Platforms (CSPs) are defined as central hubs of digital service infrastructures aiming to ensure trans-European connectivity, access and interoperability, and which are open to Member States and may be open to other entities and states that core service platforms shall be implemented primarily by the Union.
This part of a DSI is generally managed, implemented and operated by the European Commission and funding is mostly provided in the form of procurement of projects.
A distinction can be made between DSIs that can be applied across a very broad range of domains (referred to as building block DSIs) and those that are more relevant to a specific domain or sector (referred to as sector-specific DSIs).
An example of a building block DSI is 'cybersecurity' which provides services to enhance the EU-wide capability for preparedness, information sharing, coordination and response to cyber threats.
An example of a sector-specific DSI is eHealth which provides services enabling cross-border interactions between citizens and health care providers as well as between the health care providers.

What are Generic Services?

Generic Services are defined as gateway services linking one or more national infrastructure(s) to CSP(s) and are to be implemented by the parties connecting to the relevant CSP.
Generic services are the link between national infrastructures and the CSPs.
This part of a DSI is mainly managed, implemented and operated by the Member States, funding is mostly provided in the form of grants.

What is the CEF Cybersecurity DSI?

As defined in the CEF Work Programmes 2014 and 2015, the Cybersecurity DSI should be established to enable Europe to make full use of its collective capabilities to improve cybersecurity through timely and effective collaboration between the Member States.

The overall objective of the Cybersecurity DSI is to prepare and facilitate the launch of a CSP, composed of cooperation mechanisms that will enhance the EU-wide capability for preparedness, cooperation and information exchange, coordination in response to cyber threats. This Cybersecurity DSI is being set up through projects and initiatives supervised by the European Commission DG CONNECT.

What is the SMART 2014/1079 project about?

The project SMART 2014/1079 performs preparatory activities for the launch of the Connecting Europe Facility (CEF) Core Service Platform for Cooperation Mechanisms for CSIRTs in the European Union. This project was launched in 2015 by the European Commission and is led by Deloitte.
The preparatory activities of SMART 2014/1079 supports the vision for the CEF Cybersecurity DSI to achieve effective and sustainable cybersecurity cooperation across borders in Europe through enhanced collective EU-wide capabilities. Such capabilities include preparedness, information sharing, coordination and aligned response to cyber threats.
So far, the preparatory activities defined the technical, organisational and functional requirements of the CSP, a CSIRTs driven governance structure, the elements of its sustainability, as well as a roadmap for the long-term operation of the platform.

...and the SMART 2015/1089 project

The SMART 2015/1089 project was also launched in 2016 by the European Commission and has as main objective to develop and implement the technology environment and software components that will support the CSP to be used by n/g CSIRTs, on a voluntary basis.

Funding via Cybersecurity Generic Services

In 2016, the CEF Cybersecurity programme[2] allocated 12 million euro of funding for activities towards increasing the preparedness of n/g CSIRTs (e.g. identification, and detection of cyber threats, cybersecurity awareness campaigns) and for the establishment of access points to the European-wide cybersecurity cooperation mechanisms (e.g. interfaces to used tools, common formats such as incident taxonomies).
The specific objective is to support Generic Services provided by n/g CSIRTs in all the Member States, building on their interoperability with the EU cooperation mechanisms (i.e. the Core Service Platform) and their services.

The n/g CSIRTs can receive funds to create, maintain or expand national capacities to run a range of cybersecurity services allowing them to interact with other n/g CSIRTs through the CSP.

What is the role of ENISA?

According to its 2017[3] Work Programme, the European Union Agency for Network and Information Security (ENISA) will support the development of cooperation procedures for the EU-level operational security networks and take on any responsibilities assigned to it in the context of the CSP which is to be developed under the CEF programme.

ENISA will prepare to manage and operate the centralised components of the CSP of the Cybersecurity DSI to be implemented during 2016-2019 under the CEF Work Programme.

Conclusion

For the first time ever, in 2017 the development of cybersecurity capabilities in the Member States will be also directly funded through CEF cybersecurity grants. A number of n/g CSIRTs have already applied in 2016 to the CEF Telecom Call - Cyber Security (CEF-TC-2016-3). Another iteration of calls are expected to be published[4] in April 2017.

Deloitte is actively supporting individual n/g CSIRTs and other competent national cyber authorities in all Member States, in order to successfully apply for the grants made available via the CEF Telecom Call - Cyber Security as well as prepare for and execute the activities planned in the applications submitted, by supporting these with Deloitte cyber security services.

For more details please contact the authors of this article.

2 https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2016-cef-telecom-call-cyber-security-cef-tc-2016-3

3 https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019/at_download/file

4 https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2016-cef-telecom-call-cyber-security-cef-tc-2016-3