European Cybersecurity Industrial, Technology & Research Competence Centre
&
Network of National Coordination Centres

Building Cybersecurity Capabilities in Europe

EU Action for Cybersecurity

Building EU Resilience to cyber attacks	Creating effective EU cyber deterrence	Strengthening international cooperation on cybersecurity
Reformed ENISA	Identifying malicious actors	Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
EU cybersecurity Certification Framework	Stepping up the law enforcement response	Advancing EU cyber dialogues
NIS Directive Implementation	Stepping up public-private cooperation against cybercrime	Modernising export controls, including for critical cyber-surveillance technologies
Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund	Stepping up political and diplomatic response	Continue rights-based capacity building model
Cybersecurity competence network with a European Cybersecurity Research and Competence Centre	Building cybersecurity deterrence through the Member States' defence capabilities	Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence
Building strong EU cyber skills base, improving cyber hygiene and awareness		

Cybersecurity Package Commitment

EUROPEAN COMMISSION

Brussels, 13.9.2017

JOIN(2017) 450 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

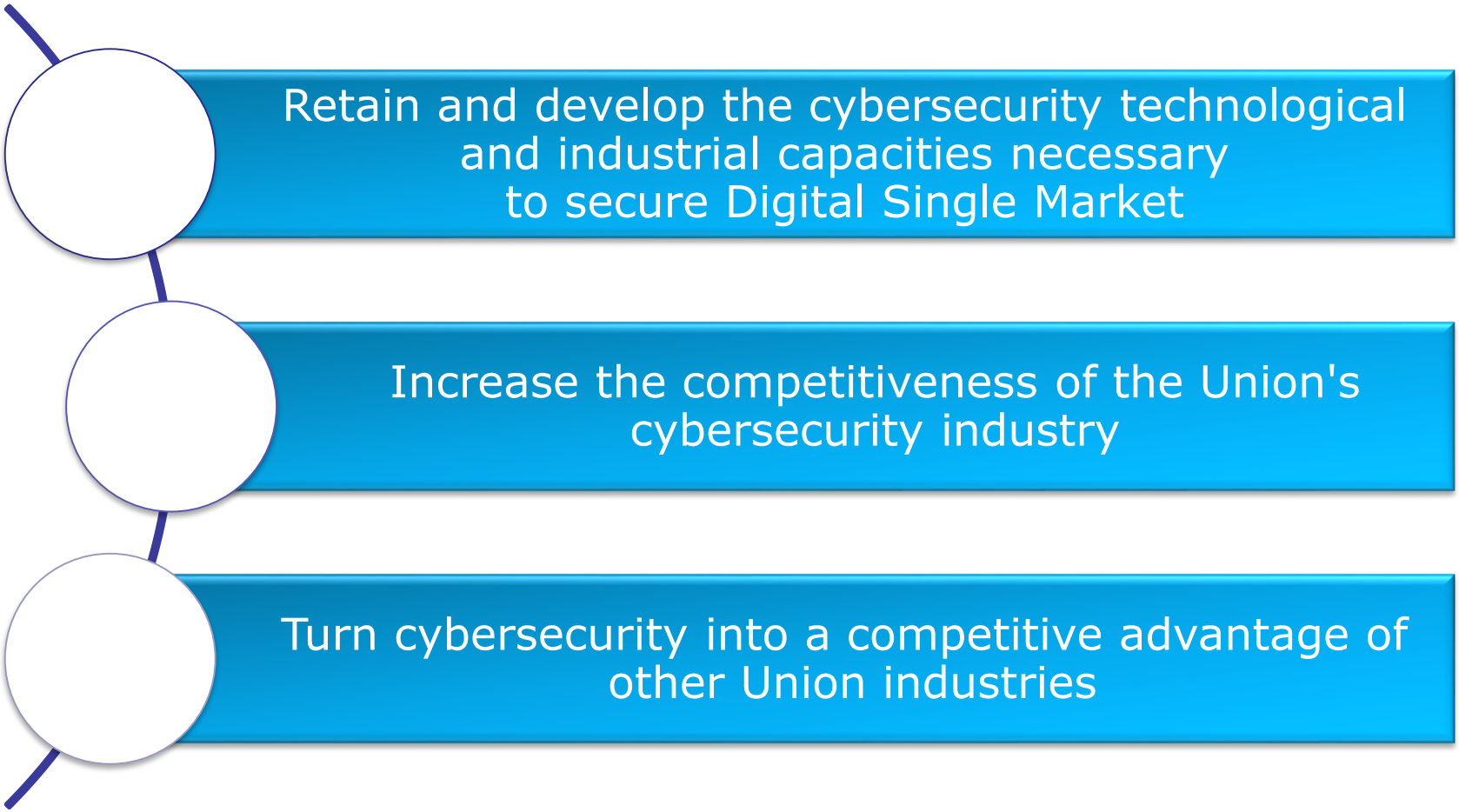
Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

The EU has added value to provide, given the sophistication of cybersecurity technology, the large-scale investment required, and the need for solutions that work across the EU.

Building on the work of Member States and the Public-Private Partnership reinforce EU cybersecurity capability through a network of cybersecurity competence centres with a European Cybersecurity Research and Competence Centre at its heart.

This network and its Centre would stimulate development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level.

A Competence Network and the Centre to…



A mechanism allowing to:

Pool, share and ensure access to existing expertise

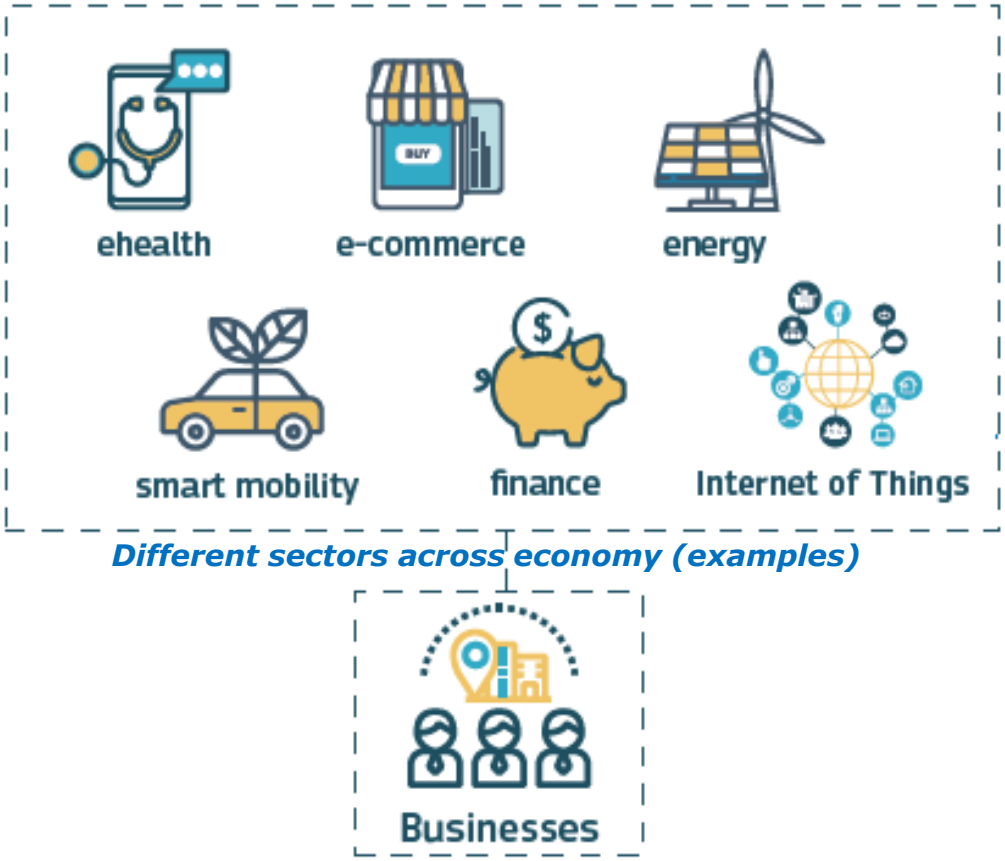
Co-invest and share costly infrastructure

Help deploy EU cybersecurity products and solutions

Ensure long-term strategic cooperation between industries, research communities and governments

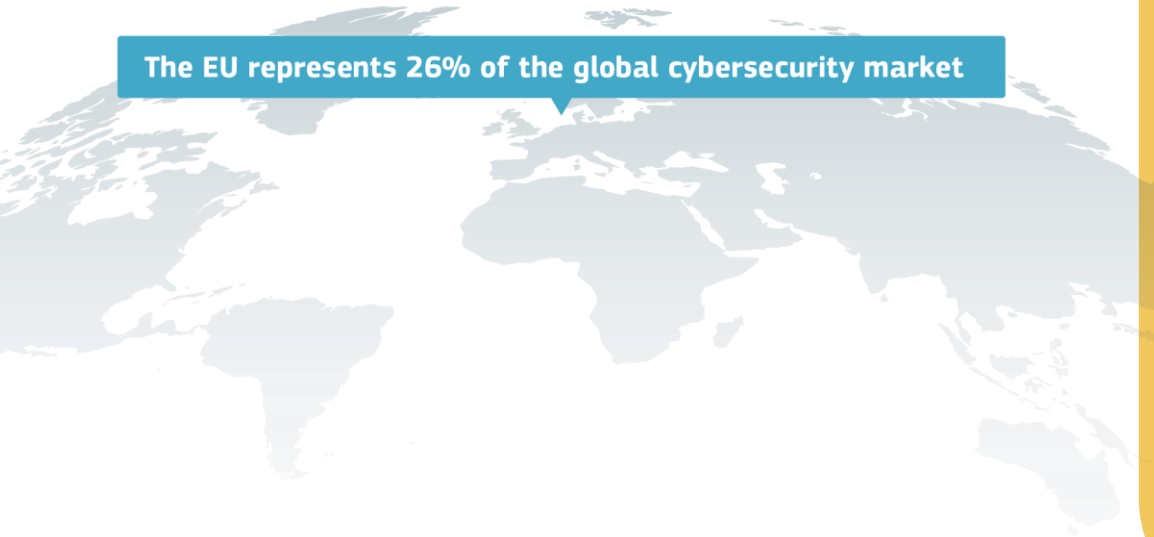
Help overcome the cyber skills gap

For the benefit of...



The situation today

Key cybersecurity technologies – where does the EU stand



CYBERSECURITY PRODUCTS AND SOLUTIONS

Up to 30% of the European demand is met by companies headquartered outside the EU.

Europe is the location for the corporate headquarters of only 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas, 7% for Israel and 4% for Asia.

A wealth of cybersecurity knowledge in Europe

More than 660 expertise centres registered in the mapping of cybersecurity centres of expertise

ECSO has +/- 240 members

ECS
EUROPEAN CYBER SECURITY ORGANISATION

European Commission

Stakeholders' expectations – what we have learnt?

Create a technology/ innovation knowledge management platform, which could be used by the whole cybersecurity community

Help close the cybersecurity skills gap and prevent brain drain by offering interesting challenges for European researchers/innovators

Help create Europe-wide cybersecurity ecosystem allowing to cooperate public authorities, industries and research communities from both civilian and military sectors

Help achieve interdisciplinary approach to cybersecurity in Europe

Ensure visibility of European cybersecurity know-how and competence both within the EU and globally

Act beyond research and development only and include also market deployment activities

Help the community work with a longer-time, strategic perspective

Key to success:

- A collaborative and inclusive approach to the Network to avoid creating new silos
- A well-defined role of the Centre
- A flexible structure easily adaptable in a fast-pace cybersecurity environment

The proposal in a nutshell

European Cybersecurity Technology & Innovation Ecosystem

European Competence Centre:

- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

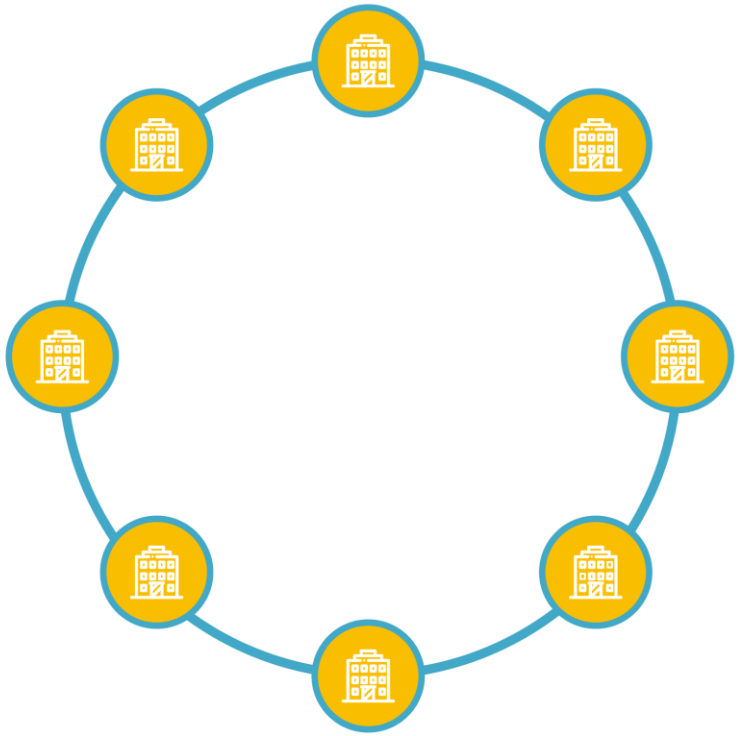
Network of National Coordination Centres:

- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors

Network of National Coordination Centres



National Coordination Centres:

- Nominated by Member States & notified to the Commission
- Possess or have access to technological expertise in cybersecurity
- Can effectively engage and coordinate with industry, academia and the public sector
- Can receive direct grants
- Can provide financial support to third parties

Tasks of the National Coordination Centres

Cybersecurity Competence Community

Academic and research organisations

Industry (demand and supply)

Public Authorities

Other stakeholders

Union bodies with relevant experience

Relevant Associations

An open and diverse group of actors involved in cybersecurity technology

Expertise in research, industrial development or training and education required

Assessment done by the Member State where the entity is established and then accredited by the Competence Centre

Only entities established within the Union may be accredited

Cybersecurity Competence Community

Academic and research organisations

Industry (demand and supply)

Public Authorities

Other stakeholders

Union bodies with relevant experience

Relevant Associations

Support the Centre and the Network in achieving the mission and objectives

Enhance and disseminate cybersecurity expertise across the Union

Participate in activities promoted by the Network and the Centre

Participate in the working groups on specific activities

Promote the outcomes of specific projects

The Competence Centre – what will it do?

Facilitate and help coordinate the work of the Network

Implement cybersecurity parts of Digital Europe and Horizon Europe Programmes

Enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities

Contribute to the wide deployment of state-of-the-art cyber security products and solutions across the economy

Contribute to reducing skills gaps in the Union related to cybersecurity

Contribute to the reinforcement of cybersecurity research and development

Enhance cooperation between the civilian and defence spheres with regard to dual use technologies and applications

Enhance synergies between the civilian and defence dimensions of cybersecurity in relation to the European Defence Fund

Preparatory work: pilot

SU-ICT-03-2018 - Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

Participants should in parallel propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub.

Projects under this topic will help build and strengthen cybersecurity capacities across the EU as well as provide valuable input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre as mentioned by the Joint Communication *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,* JOIN (2017) 450 final.

Next Steps

European Commission

By Q2/2019

Finalise negotiations

2019-2020

Preparatory Phase

2020

Prepare to launch 2021 actions

Funding opportunities in H2020 and Connecting Europe Facility

EU Contribution to Cybersecurity and digital privacy

European Commission

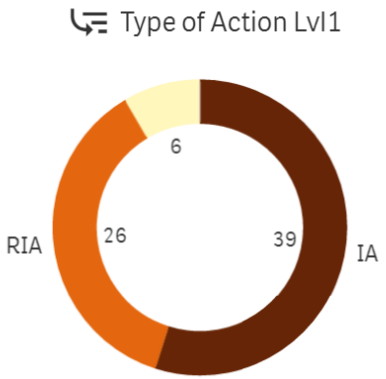
H2020 Signed Grants

71 0,35% of H2020

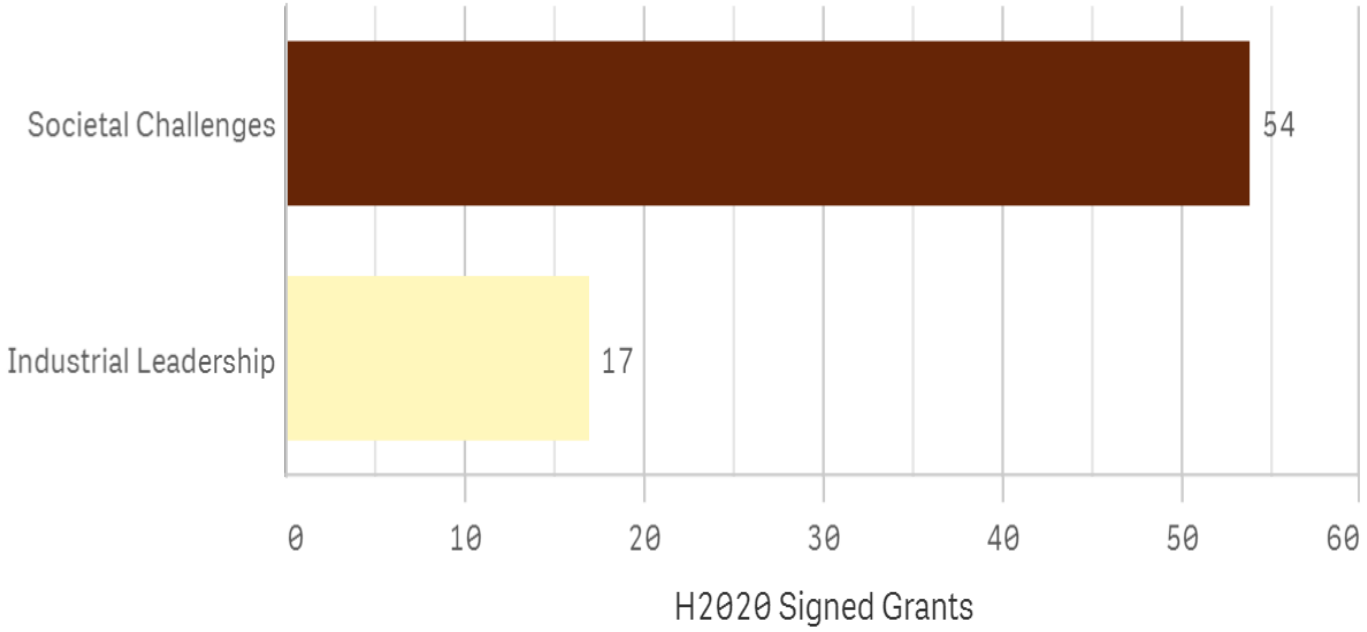
H2020 EU Contribution

260M 0,74% of H2020

Signed Grants by Type of Action



Signed Grants by Pillar / Thematic Priority



Top Topics

Topic	Topic Descr	H2020 Signed Grants	H2020 EU Contribution
Totals		**71**	**€ 260.037.709**
ICT-32-2014	Cybersecurity, Trustworthy ICT	10	€ 38.578.248
DS-01-2016	Assurance and Certification for Trustworthy and Secure ICT systems, services and components	7	€ 23.486.256
DS-08-2017	Cybersecurity PPP: Privacy, Data Protection, Digital Identities	7	€ 19.693.593
DS-07-2017	Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors	6	€ 20.743.593
DS-01-2014	Privacy	6	€ 19.578.047
DS-04-2015	Information driven Cyber Security Management	5	€ 20.302.856
DS-02-2016	Cyber Security for SMEs, local public administration and Individuals	5	€ 18.977.175
DS-02-2014	Access Control	4	€ 19.483.908
DS-06-2017	Cybersecurity PPP: Cryptography	4	€ 19.116.918
DS-03-2015	The role of ICT in Critical Infrastructure Protection	3	€ 16.991.061
DS-06-2014	Risk management and assurance models	3	€ 10.272.197
DS-04-2016	Economics of Cybersecurity	3	€ 5.989.903

Cybersecurity as a significant share of other calls

For example:

Half of the EU Contribution to topic CIP-01-2016-201 is Cybersecurity funding:

H2020 Signed Grants	H2020 EU Contribution
6 0,03% of H2020	45,78M 0,13% of H2020

Topic	Topic Descr
Totals	
CIP-01-2016-2017	Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of

H2020 budget foreseen 2018-2020

H2020 EU Contribution/Budget CyberSecurity plus Digital privacy	2018	2019	2020	Grand Total
Industrial Leadership	90	56	47	193
Call - Cybersecurity	90	15	47	152
Call - Information and Communication Technologies		41		41
Future Emerging Technologies	10			10
FET FLAGSHIPS – Tackling grand interdisciplinary science and technology challenges	10			10
Societal Challenge 1 - Health, demographic change and wellbeing	36			36
Call - Trusted digital solutions and Cybersecurity in Health and Care	36			36
Societal Challenge 7 - Secure Societies	54,5	58	78,8	191,3
Call - Digital Security	44,5	38	68,8	151,3
Call - INFRA	10	20	10	40
Grand Total	190,5	114	125,8	430,3

H2020 budget foreseen 2018-2020

H2020 EU Contribution/Budget CyberSecurity plus Digital privacy	2018	2019	2020	Grand Total
Industrial Leadership	**90**	**56**	**47**	**193**
Call - Cybersecurity	**90**	**15**	**47**	**152**
SU-ICT-01-2018 : Dynamic countering of cyber-attacks	40			40
SU-ICT-02-2020 : Building blocks for resilience in evolving ICT systems			47	47
SU-ICT-03-2018 : Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap	50			50
SU-ICT-04-2019 : Quantum Key Distribution testbed		15		15
Call - Information and Communication Technologies		**41**		**41**
ICT-08-2019 : Security and resilience for collaborative manufacturing environments		11		11
ICT-09-2019-2020 : Robotics in Application Areas		10		10
ICT-13-2018-2019 : Supporting the emergence of data markets and the data economy		10		10
ICT-20-2019-2020 : 5G Long Term Evolution		10		10

H2020 budget foreseen 2018-2020

H2020 EU Contribution/Budget CyberSecurity plus Digital privacy	2018	2019	2020	Grand Total
Industrial Leadership	**90**	**56**	**47**	**193**
Future Emerging Technologies	**10**			**10**
FET FLAGSHIPS – Tackling grand interdisciplinary science and technology challenges	**10**			**10**
Societal Challenge 1 - Health, demographic change and wellbeing	**36**			**36**
Call - Trusted digital solutions and Cybersecurity in Health and Care	**36**			**36**
Societal Challenge 7 - Secure Societies	**54,5**	**58**	**78,8**	**191,3**
Call - Digital Security	**44,5**	**38**	**68,8**	**151,3**
SU-DS01-2018 : Cybersecurity preparedness - cyber range, simulation and economics	16			16
SU-DS03-2019-2020 : Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises		18		18
SU-DS04-2018-2020 : Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches	20			20
SU-DS05-2018-2019 : Digital security, privacy, data protection and accountability in critical sectors	8,5	20		28,5
Other TBC (2020) :			68,8	68,8
Call - INFRA	**10**	**20**	**10**	**40**
SU-INFRA01-2018-2010-2020 : Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	10	10		20
SU-INFRA02-2019 : Security for smart and safe cities, including for public spaces		10		10
Other TBC (2020) :			10	10
Grand Total	**190,5**	**114**	**125,8**	**430,3**

Connecting Europe Facility: Support for NIS implementation

Connecting Europe Facility (CEF) 2018 Call: 13mEUR envelope

Capabilities Development

- Infrastructure & Skills
- Structural Supports

Prospective Applicants

- National CSIRTs – designated by MS under NIS Directive
- OES –identified by MS under the Directive
- DSPs – in line with NIS Directive
- Cooperative, Connected & Automated Mobility (CCAM)
- SPOCs and National Competent Authorities
- Public Bodies

Long open period: 16th May to 22nd November