Benchmarking report on Cybersecurity and Privacy landscape in EU and US

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission´s behalf may be held responsible for the use which may be made of the information contained therein.

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CSA	Coordination and Support Action
CSP	cybersecurity and privacy
R&I	Research and Innovation
ICT	Information and Communication Technology
IT	Information Technology
CSA	Coordination and Support Action
NITRD	Networking and Information Technology Research and Development Program
SaCT	Secure and Trustworthy Cyberspace
NSF	National Science Foundation
DHS	Department of Homeland
SCIA	Cybersecurity and information assurance
DoD	Department of Defence
NSTC	National Science and Technology Council
DARPA	Defense Advanced Research Project Agency
IARPA	Intelligence Advanced Research Projects Activity
NIS	Network and Information Security
cPPP	Contractual Public Private Partnership
ECSO	European Cyber Security Organisation
SRA	Strategic Research Agenda
SRIA	Strategic Research and Innovation Agenda
ENISA	The European Union Agency for Network and Information Security
IoT	Internet of Things

EXECUTIVE SUMMARY

The AEGIS Project, a Coordination and Support Action (CSA) project funded by Horizon 2020 (the EU Framework Programme for Research and Innovation) aims to facilitate EU-US dialogue and cooperation in cybersecurity and privacy research and innovation (R&I). The project has developed this deliverable in an attempt to capture the current landscape of R&I in cybersecurity and privacy on both sides of the Atlantic.

This deliverable provides the analysis of EU and US cybersecurity and privacy R&I priorities. The analysis is based on the main documents that highlight the most important areas for R&I and funding programmes. We compare the results of this desktop analysis with the results of our "Identification of EU-US Priorities for EU-US Cooperation" survey, which was carried out in May 2018. The results of the survey are published in D3.1. Additionally, we provide similar insights from a researcher´s perspective.

We have found that cybersecurity technology topics such as *Security Management and Governance; Data Security and Privacy; Education and Training; Assurance, Audit, and Certification;* and *Network and Distributed Systems* get the most attention from the funding programme managers as well as from researchers. *Internet of Things* (*IoT*) has been found to create the most demanding cybersecurity and privacy challenges among ICT technologies, followed by *Cloud, Mobile, Big Data*, and *Operating Systems*. The Application domains, meanwhile, are dominated by *Energy, Public Safety, Transportation, Financial Services* and *Healthcare.* In general, these results coincide well with the results of our online survey.

We have applied the results of the analysis to the three AEGIS focus application domains, Healthcare, Financial and Maritime, to find out how well the most important CSP issues in all three domains are addressed by current R&I priorities. Our analysis shows that most of the high priority areas are well covered by the available programmes. Nonetheless, *Cryptography* has received less attention than the demand side requires. In addition, the EU has put more emphasis on topics such as *Assurance, Audit and Certification* and *Trust Management, Assurance, and Accountability*, while US devotes little attention to these topics. For *Identity and Access Management* and *Software and Hardware Security Engineering*, the situation is opposite.

Finally, the deliverable provides several recommendations for the future EU-US collaboration in R&I for cybersecurity and privacy.

1 INTRODUCTION

The European Union (EU) and the United States (US) have their own long running research and innovation (R&I) funding programmes for cybersecurity and privacy. The biggest current EU R&I funding programme is Horizon 2020 (with nearly €80 billion of funding available, in total) has several calls related to cybersecurity (H2020-SU-ICT-2018-2020[1]). In the United States, several agencies (including, the well-known DARPA agency, NSF, NIST, etc.) have their own funding programmes, which also fund cybersecurity and privacy (CSP) research. The programmes aim to cover the most important cyber security areas which, according to each funding agency, should have the biggest and the most influential impact on economy, industry and society.

The effect of the development of information technology (IT) and its rapid penetration and reshaping of the modern industry and society is, to the large extent, similar on the both shores of the Atlantic and both EU and US face similar cybersecurity and privacy challenges, which require additional research and innovation ideas. Thus, it is not very surprising that different CSP funding programmes have similar focus areas. At the same time, for the funding programme developers it is important to understand where the research focus of EU and US coincide, i.e., acknowledged by both unions as a promising topic, and where the focus diverge, which could mean either an excessive funding of the area by one side or underfunding of an important area by another (or both). Naturally, different legal, political and business landscapes have their influence on shaping the prioritized areas for research and this also has to be taking into account in while confronting different programmes.

Finally, not only the lessons can be learnt out of the analysis of different priorities of EU and US; facing similar challenges should lead us to uniting forces for approaching the problems and looking for the most appropriate solutions by bringing together the excellence from both shores of the Atlantic. In other words, we should look for the areas where fostering EU-US collaboration will lead to the most fruitful results.

The AEGIS Project, a Coordination and Support Action (CSA) project funded by Horizon 2020 (the EU Framework Programme for Research and Innovation) aims to facilitate EU-US dialogue and cooperation in cybersecurity and privacy research and innovation (R&I). The project has developed this deliverable in an attempt to capture the current landscape of R&I in cybersecurity and privacy on both sides of the Atlantic.

This deliverable provides the analysis of EU and US cybersecurity and privacy R&I priorities. The analysis is based on the main documents that highlight the most important areas for R&I and funding programmes. We compare the results of this desktop analysis with the results of our "Identification of EU-US Priorities for EU-US Cooperation" survey, which was carried out in May 2018. We have applied the results of the analysis to the three AEGIS focus application domains, Healthcare, Financial and Maritime, to find out how well the most important CSP issues in all three domains are addressed by current R&I priorities. Finally, the deliverable provides several recommendations for the future EU-US collaboration in R&I for cybersecurity and privacy.

[1] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-su-ict-2018-2020.html

1.1 Overall Methodology

The following methodology was applied for the identification of CSP R&I priorities of EU and US

1) *Identification of the relevant document*
   We have identified the documents which influence the most CSP R&I priorities of EU and US. We also looked into the concrete CSP R&I programme implementations of various funding agencies, if such documents are available.
2) *Desktop analysis*
   We analysed the identified documents, paying specific attention to the Cybersecurity Processes, ICT domains, and Applications of the JRC's taxonomy, which is adopted for the landscape analysis in our project (see Deliverables 2.1 and 2.2 for more details). In short, we identified the areas of the JRC taxonomy, which are prioritised by every identified document. Finally, we aggregated the results (taking into account the degree of importance of every analysed document) to get the overall results for EU and US
3) *Programme developers vs. researchers*
   The results of the desktop analysis are merged with the results of the survey conducted by AEGIS project (see Deliverable 3.1). The survey provides the views of researchers on the CSP R&I topics which require more attention.
4) *Analysis of the application needs*
   We have identified the needs of the three focus applications: Healthcare, Financial, and Maritime, and analysed which topics have got enough attention from existing programmes and which need additional funding.
5) *Recommendations for collaboration*
   First, we analysed other EU-US collaborating projects to see which recommendations have been drawn by previous collaborating efforts. Then, we provided several our recommendations, which should help to strengthen the research cooperation between countries.

1.2 Target Audience

The target audience of this deliverable is R&I funding programme managers who would like to understand the trends in cybersecurity and privacy research and innovation across the Atlantic and shape their programmes according to research interests. It is also aimed at researchers from both academia and the industry who would like to identify prominent directions in research and identify fruitful areas for collaborations.

2 EU/US PRIORITIES FOR R&I IN CYBERSECURITY AND PRIVACY

In this section we analyse the priorities of EU and US with respect to coverage of various cybersecurity and privacy topics in their future R&I programmes. We map the priorities with the cybersecurity technologies defined in WP2 and qualitatively analyse the attention devoted by EU and US to cybersecurity R&I.

2.1 Methodology for Desktop Analysis

The methodology for our desktop analysis is the following. First, we have defined a taxonomy for analysis of CSP landscape. We have devised our own taxonomy (which can be found in the Appendix), splitting apart cybersecurity Technology topics, ICT technology topics, and Application domains that require specific attention of cybersecurity. While we were working on our taxonomy we have found that Joint Research Council is working on their own taxonomy (see Section 2.2), which is going to be used by the European Commission in the future. We have decided to use the new JRC Taxonomy[2] to facilitate further integration of our results in the future programmes of the European Commission.

Then, a number of the most influential documents for the R&I programmes of the EU and US have been identified. For both EU and US, we have found strategic R&I plans issued by the higher governmental structures; as well as concrete programmes descriptions and the Research Strategic Agendas which have been used for specification of these programmes. A weight has been assigned to every document according to its influence on the R&I programmes.

For every category of the selected taxonomy we identified the topics which have got most attention in the considered document. In most cases, these are the topics explicitly listed in the documents (e.g., a list of prioritised cybersecurity technologies), but some applications and ICT technology topics were added after analysis of the documents on the basis of amount of attention devoted to them. For some documents we were not able to find an explicit list of the prioritised topics (e.g., for DHS in US or ENISA in EU), but we were able to use the structure of the programmes/initiatives instead to single out the prioritised directions. For some documents we were not able to identify either ICT Technology topics or Application domains, as the considered document simply does not focus on them. We excluded such documents from the consideration of ratings of topics for the corresponding domains (we simply assigned weight 0 to the document in such cases). After the analysis, we have got ratings (a value from 0 to 1) for every topic for the three considered vectors.

2.2 JRC Taxonomy

In this section we briefly summarize the JRC's taxonomy (the one used in this paper[3]) applied for our landscape benchmarking analysis.

The JRC's taxonomy defines three vectors for categorising CSP R&I directions. Note that we use slightly different names of the three vectors.

- Cybersecurity Research Domains;

[2] At the time the work on the document was performed the JRC's taxonomy was in a draft state (Version 3.0). The final published version can be found here: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf

[3] Note that the final version of the JRC's taxonomy is slightly different, but the changes are negligible with respect to the version we are using in this document.

- Application and Technologies;
- Sectors.

Cybersecurity Research Domains include technical cybersecurity topics related to specific cybersecurity technologies. In our analysis we refer to these areas as "*Cybersecurity Technology Topics*". The Application and Technologies vector includes the topics on various "*ICT Technologies*" (such as the Cloud, IoT, Big Data, etc.) which require cybersecurity protection. Sectors are the "*Applications*" (e.g., Healthcare, Maritime, Energy, etc.) in which the cybersecurity technologies are applied and contextualised.

The Cybersecurity Technologies are broken into the following topics:

- **Assurance, Audit, and Certification**
  This topic includes the methodologies, frameworks and tools for providing the confidence that the system or a network is operating as designed with respect to the security goals and according to the security policies.
- **Cryptology (Cryptography and Cryptanalysis)**
  This topic includes the mathematical and algorithmic aspects of cryptography, its technical and architectural implementation, as well as the cryptanalytic methodologies, techniques and tools.
- **Data Security and Privacy**
  This topic includes the issues related to reduction (by design) privacy and confidentiality risks for data or preventing its misuse by authorized entities.
- **Education and Training**
  This topic includes techniques and tools for acquiring knowledge, know-how, skills and competence required for protection of network and information systems, their users and clients from cyber threats.
- **Operational Incident Handling and Digital Forensics**
  This topic includes the theories, techniques, tools and processes for the identification, collection, acquisition and preservation of digital evidence of incidents.
- **Human Aspects**
  This topic includes the issues related to cybersecurity ethics, relevant laws, regulations, policies, standards, psychology of human beings within the cybersecurity realm.
- **Identity and Access Management**
  This topic includes authentication, authorization and access control of individuals and smart devices when accessing resources.
- **Security Management and Governance**
  This topic includes activities, methodologies, processes and tools for governance and management of cybersecurity.
- **Network and Distributed Systems**
  This topic includes the issues related to secure integration and communication of hardware and software within a scope of a network system.
- **Software and Hardware Security Engineering**
  This topic includes techniques, tools and methodologies for securing software and hardware during the whole development lifecycle, including risk and requirements analysis, architecture design, code implementation, validation, verification, testing, deployment and runtime monitoring of operation.
- **Security Measurements**
  This topic includes the techniques, tools and methodologies for facilitation of analysis, decision making and reporting of cybersecurity performance-related data.

- **Legal Aspects**
  This topic includes legal and ethical aspects related to the misuse of technology, abuse of intellectual property rights illicit distribution and/or the enforcement of law related to cybercrime and digital rights.
- **Theoretical Foundations**
  This topic includes the formal analysis and verification techniques to gain theoretical proof of security properties in software, hardware, and algorithm design.
- **Trust Management, Assurance, and Accountability**
  This topic includes techniques, tools and methodologies for management of trust related to digital and physical entities, e.g., applications, services, components, or systems.

Difference with the final version of JRC taxonomy. The final version of the JRC taxonomy has the same list of Cybersecurity Technologies.

The ICT Technologies domain contains the following topics:

- **Information Systems**
- **Mobile Devices**
- **Operating Systems**
- **Big Data**
- **Vehicular Systems**
- **Critical Infrastructures**
- **Industrial Control Systems**
- **Supply Chain**
- **Internet of Things**
- **Hardware**
- **Cloud and Virtualization**
- **Pervasive Systems**
- **Embedded Systems**

Difference with the final version of JRC taxonomy. The final version of the taxonomy includes the following additional topics: *Quantum technologies; Artificial Intelligence; Robotics Blockchain & Distributed Ledge Technologies; High Performance Computing; Satellite systems; Human Machine Interface*. It also excludes *Critical Infrastructure* from the list.

The Application domain has the following topics:

- **Defence**
- **Energy**
- **Financial Services**
- **Health**
- **Industry 4.0**
- **Nuclear**
- **Public Safety**
- **Supply Chain**
- **Telecom**
- **Transportation**
- **Water**

Difference with the final version of JRC taxonomy. The final version of the taxonomy includes the following additional topics: *Audio visual and media; Digital Infrastructure; Governmental and public authorities; Maritime; Tourism; Smart*

Ecosystems; Space. It also excludes the following three topics from the list: *Telecommunication*[4]*; Water; Industry 4.0.*

2.3 Desktop Analysis

2.3.1 US

US priorities in cybersecurity are shaped by many publications and initiatives. This is partly due to the fact that policymaking in the country is a multi-layered process made up of many agencies and initiatives. The following documents have been selected for analysis:

- US Report of the United States President's Commission on Enhancing National Cybersecurity[5] on the 1st December, 2016;
- Federal Cybersecurity Research and Development Strategic Plan[6] (released in December 2016);
- Secure and Trustworthy Cyberspace programme[7] (SaTC) of National Science Foundation (NSF);
- Cyber Security Division[8] (CSD) programme of Department Homeland Security (DHS);
- DARPA programmes[9];
- IARPA programmes[10].

The report produced by the United States President's Commission on Enhancing National Cybersecurity includes a number of recommendations established by the US President for cybersecurity, which served as a goal setting guideline for agencies to determine priorities and plans for their programmes. **The Federal Cybersecurity Research and Development Strategic Plan** was published in 2016 by the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development Program (NITRD) to implement the recommendations from the United States President's Commission on Enhancing National Cybersecurity report via a more detailed plan for R&I.

Recently, a new National Cybersecurity Strategy[11] has been released by President Donald Trump's administration, which sets new goals and objectives for the advancement of cybersecurity in US. We acknowledge its importance for the future focus of US R&I, but it is still too early to know what effect it will have on cybersecurity-related programmes (and on the NITRD program) at the moment. Anyway, we may single out the topics emphasised in the strategy, which will impact the US R&I priorities in the future. The strategy emphasises the importance of risk management (*Security Management and Governance* cybersecurity technology topic) and supply chain protection (*Supply chain* ICT technology topic) for the information security to balance potential losses and costs. The importance of security critical

[4] This topic is included into Digital Infrastructure.

[5] 1st December, 2016, Final; report of the United States Presidents Commission on Enhancing National Cybersecurity https://www.nist.gov/cybercommission. The report was produced by the commission established by the former US President Barack Obama, but it is still relevant and is included in this document.

[6] https://www.nitrd.gov/pubs/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

[7] https://www.nsf.gov/pubs/2017/nsf17576/nsf17576.pdf

[8] https://www.dhs.gov/science-and-technology/csd-projects

[9] https://www.darpa.mil

[10] https://www.iarpa.gov/

[11] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

infrastructures is also highlighted in the document. In particular, the document singles out the *Transportation*, *Maritime* and *Space* application domains. We also would like to underline that many points specified in the document are in line with the recommendations of AEGIS (see Section 2.6). In particular, the document underlines the importance of Education, Securing Critical Infrastructure, and International collaboration (as with incidence reporting and fighting cybercrime, as well is in protecting freedom in the Internet).

NITRD coordinates different agencies and provides a platform for them to exchange experience and views. In this way, it provides an aggregated view of different agencies on cybersecurity and privacy issues. NITRD's website[12] contains information about the investments of different agencies in cybersecurity and information assurance.

Table 1: R&I programmes in cybersecurity and privacy budget

Agency	Budget, $ in Millions
DARPA	301,90
DHS	43,90
DOE	30,00
DoD	206,20
NIH	3,60
NIST	59,70
NSF	98,50

As shown in Table 1 (and on the pie graph in Figure 1), DARPA and the Department of Defence (DoD) invest more in cybersecurity, which is understandable since both agencies are military driven. It is not possible to obtain more details on the DoD's funding programmes, as more information is not available for the general public, but DARPA's funded programmes are available for reference through its the website. The **National Science Foundation** (NSF) and **Department of Homeland Security** (DHS) make significant investments in cybersecurity and privacy R&I and have detailed research programmes available. Therefore, they are also considered in our analysis.

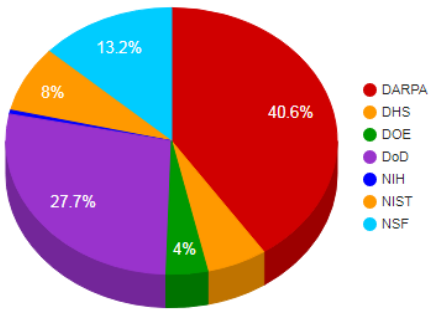


Figure 1: A pie-graph of US cyber security budget distribution in 2018

2.3.1.1 Report of the United States President's Commission on Enhancing National Cybersecurity

The **Commission on Enhancing National Cybersecurity**, established by the US President Barack Obama, produced a final report[13] containing the recommendations for securing and growing the digital economy by strengthening cybersecurity in the

[12] https://www.nitrd.gov/apps/itdashboard/Dashboard.aspx

[13] 1st December, 2016, Final; report of the United States Presidents Commission on Enhancing National Cybersecurity https://www.nist.gov/cybercommission.

public and private sectors. The commission initially identified eight cybersecurity topics to study and, then, added two more. These topics are:

- federal governance
- critical infrastructure
- cybersecurity research and development
- cybersecurity workforce
- identity management and authentication
- Internet of Things
- public awareness and education
- state and local government cybersecurity
- insurance
- international issues

Also, the commission took into account other trends and issues affecting the mentioned topics, such as the convergence of information technologies and physical systems, risk management, privacy and trust, global versus national realms of influence and controls, free market and regulatory regimes and solutions, legal and liability considerations, the difficulty in developing meaningful metrics of cybersecurity, and automated technology–based cybersecurity approaches and consumer responsibilities.

The commission stated it clearly and provided a number of recommendations that cyber security issues should be approached by the joined force of private and public economy sectors. The document underlines the need for usable, affordable, privacy-protecting, resilience, functional and defensive products and systems.

2.3.1.2 Federal Cybersecurity Research and Development Strategic Plan

The **National Science and Technology Council (NSTC)** and the **Networking and Information Technology Research and Development (NITRD)** released the Federal Cybersecurity Research and Development Strategic Plan[14] on the 5th of February 2016. NSTC has the primary goal to establish the national goals for Federal science and technology investment. This strategic plan substitutes the previous Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (released in December 2011). The new plan extends the set of interrelated breakthrough objectives for Federal agencies from the previous plan, expands the priorities and adds the focus on evidence-validated R&D.

As prioritised research challenges, the new strategic plan puts forward the following ones:

- **Deter**
  - Measurement of adversary level of effort, results, and risks;
  - Effective and timely attribution;
  - Robust investigative tools;
  - Information sharing for attribution;
- **Protect**
  - Design for security;
  - Build secure;
  - Verify security;
  - Maintain security;
  - Verify authenticity;
  - Authenticate users and systems;
  - Access controls;

[14] https://www.nitrd.gov/pubs/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

  - Cryptographic mechanisms to data;
  - Mitigate vulnerabilities;
- **Detect**
  - Enable robust situational awareness;
  - Identify weaknesses in systems;
  - Reliably detect malicious cyber activities;
- **Adapt**
  - Dynamic assessment;
  - Adaptive response;
  - Coordination at multiple scales.

The strategic plan also underlines the importance of the following application areas:

- Cyber-Physical Systems and the Internet of Things
- Cloud Computing
- High Performance Computing
- Autonomous Systems
- Mobile devises

2.3.1.3 NSF SaTC

National Science Foundation (NSF) runs the **Secure and Trustworthy Cyberspace** programme, aligned with the Federal Cybersecurity Research and Development Strategic Plan and the National Privacy research Strategy. The goal of the programme is to protect and preserve the benefits of computer systems by improving their security and privacy. The recent programme solicitation NSF 17-576[15] requires the proposals to be submitted to one of the following four designations:

- Secure and Trustworthy Cyberspace core research (CORE) aimed for foundational research in security and privacy
- Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) focusing on security of hardware systems.
- Transition to Practice (TTP) having the main goal to support the development, implementation, and deployment of later-stage and applied security or privacy research into an operational environment.
- Cybersecurity Education (EDU) devoted to the cybersecurity educational topics.

In particular, CORE designation specifies the following topics of interest:

- Access control and Identity Management
- Authentication and Biometrics
- Cryptography Applied and theory
- Cyber-Physical systems
- Data science
- Forensics
- Formal methods and language-based techniques
- Hardware security architecture
- Hardware security design
- Information Trustworthiness
- Intrusion Detection
- Mathematics and statistics
- Networks
- Privacy
- Social, Behavioural and Economic Sciences
- Software security engineering

[15] https://www.nsf.gov/pubs/2017/nsf17576/nsf17576.pdf

- Systems
- Usability and Human Interaction

2.3.1.4 NHS CSD

Cyber Security Division (CSD) of **Department Homeland Security (DHS)** leads federal efforts in funding cybersecurity R&D projects[16]. CSD funds a number of cybersecurity projects aiming to improve security in Federal networks as well as in the Internet. It covers the following areas:

- Anonymous Networks & Currencies
- Application of Network Measurement Science
- Critical Infrastructure Design and Adaptive Resilient Systems
- Cyber Risk Economics (CYRIE)
- Cyber Physical Systems Security (CPSSEC)
- Cyber Security Forensics
- Cybersecurity Competitions
- Cybersecurity for Oil & Gas Systems (COGS)
- Data Privacy Technologies
- Distributed Denial of Service Defense (DDoSD)
- Federated Security
- Experimental Research Testbed (DETER)
- Homeland Open Security Technology (HOST)
- Identity Management
- Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT)
- Insider Threat
- Mobile Application Security
- Mobile Device Security
- Next Generation Cyber Infrastructure Apex
- Smart Cities
- Software Assurance Marketplace (SWAMP)
- Software Quality Assurance
- Static Analysis Tools Modernization Project (STAMP)
- Transition to Practice (TTP)

2.3.1.5 DARPA

Defense Advanced Research Project Agency (DARPA[17]) is a well-known agency that, although aims for improving US military capabilities, also provides important contribution to civilian society (e.g., the Internet, automated voice recognition and language translation, Global Positioning System, etc.). DARPA aims for the transforming revolutionary concepts and tries to bring seeming impossibilities into practical capabilities. It has a constant focus on the US Nation's military Services, but also works with academic, corporate and governmental partners.

Unlike NSF or NHF, DARPA does not have a publicly available global strategic plan specified for cybersecurity and privacy, but it works with NITRD and their specific programmes for cybersecurity are publicly available at the web-site. We were able to single out 15 programmes which could be related to cybersecurity and privacy:

- active social engineering defense (ASED)
- clean-slate design of resilient, adaptive, secure hosts (crash)
- computers and humans exploring software security (chess)
- configuration security (consec)

[16] https://www.dhs.gov/science-and-technology/csd-projects

[17] https://www.darpa.mil

- cyber assured systems engineering (case)
- cyber fault-tolerant attack recovery (cfar)
- cyber grand challenge (cgc)
- cyber-hunting at scale (chase)
- edge-directed cyber technologies for reliable mission communication (edgect)
- enhanced attribution
- extreme ddos defense (xd3)
- harnessing autonomy for countering cyberadversary systems (haccs)
- high-assurance cyber military systems (hacms)
- leveraging the analog domain for security (lads)
- mission-oriented resilient clouds (mrc)
- rapid attack detection, isolation and characterization systems (radics)
- safeware
- space/time analysis for cybersecurity (stac)
- transparent computing
- vetting commodity it software and firmware (vet)
- brandeis

We see that all these programmes are much more narrow that the directions and categories singled out by other funding agencies and research agendas/plans. After a close analysis we have found that many of the programmes have a goal to harden the developed software in one way or another to make them more robust against attacks (e.g., CLASH, CHESS, CGC, SAFEWARE, etc.). There are also several projects targeting security of networks (e.g., CLASH, CONSEC, EDGECT) and improve security management and governance (e.g., CFAR, ENHANCED ATTRIBUTION, XD3, HACCS). Other security topics have much fewer (in any) programmes dedicated to them. Most programmes are generic, but some focus on a specific ICT technology (e.g., HACMS or MRC) or application domain (e.g., RADICS).

2.3.1.6 IARPA

The **Intelligence Advanced Research Projects Activity (IARPA**)[18] directs its investments in high-risk, high-payoff research programmes in the Intelligence Community. The activity addresses cross-agency challenges, leverages operational and R&D expertise in the area of Intelligence Community, and coordinates transition strategies with partner agencies. Currently, the agency has three programmes primarily targeting cybersecurity:

- CAUSE aims to develop new methods for forecasting and detection of cyber attacks earlier than current methods.
- VirtUE aims to define and develop secure cloud infrastructure and leverage these environments to detect and deter security threats for it.
- TIC aims to develop and demonstrate split-manufacturing, a new approach to chip fabrication assuring security and intellectual property protection.

2.3.2 EU

Compared to the US, the EU's R&I activities on cybersecurity are more limited to concrete actions (versus a variety of publications and programs). AEGIS has selected the following EU initiatives to analyse the prioritised directions for R&I in the field of cybersecurity and privacy. These initiatives have been selected on the basis of their influence in Europe. It is worth noting that AEGIS partners play a significant role in the majority of them.

[18] https://www.iarpa.gov/

- Horizon 2020 R&I Funding Program[19];
- The Network and Information Security Platform initiative[20];
- Contractual PPP on cybersecurity [21] (cPPP) and its supporting organisation European Cyber Security Organisation[22] (ECSO) initiative;
- The activities of the European Union Agency for Network and Information Security[23] (ENISA).

Horizon 2020 is the largest European R&I funding programme. It has a budget of approximately €80 billion available for 7 years (from 2014 to 2020) in addition to private investments. As a guiding principle, H2020 aims to increase the number of innovation breakthroughs, discoveries and world-firsts by helping take ideas from the research lab to the market.

In the scope of the Horizon 2020 programme, the most recent call on cybersecurity was *H2020-SU-ICT-2018-2020,* which closed in August 2018. The call underlines the importance of cybersecurity for European digital economy and encourages European industry players, services and products to comply with the current EU regulations and directives, such as the **NIS Directive[24]**, eIDAS, GDPR and Directive 95/46/EC.

The contractual **Public Private Partnership (cPPP)** in Cybersecurity was formed in July 2016. The call mentioned above acknowledges the importance of the input provided by this cPPP for H2020 WP2018-2020. The topics of the cybersecurity call are a partial contribution of the Commission to the cybersecurity cPPP.

ENISA, the **European Union Agency for Network and Information Security**, was created by Regulation (EC) No 460/2004 [25] of the European Parliament. Its mission is to help secure the European information society by raising ”awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union.” The agency releases its threat landscape about the most dangerous threats and challenges annually and structures its activities according to the most important cybersecurity topics.

2.3.2.1 NIS Platform

The Network and Information Security Public Private Platform[26] (NIS Platform) was found in June, 2013, in scope of the framework of the EU Cybersecurity Strategy[27] and was coordinated by the European Commission and ENISA. The platform united the key European stakeholders from academic, research and industry who worked

[19] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-su-ict-2018-2020.html

[20] 31st December, 2015, Strategic Research Agenda Final v0.96, https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/view

[21] https://www.ecs-org.eu/cppp

[22] https://www.ecs-org.eu/

[23] https://www.enisa.europa.eu/

[24] http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm

[25] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[26] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[27] http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

together on a **strategic research agenda**[28] (SRA), released in December 2015. The SRA complemented and supported the NIS Directive (the Directive on Security of Network and Information Systems[29]) and was intended to be used by secure ICT Research & Innovation agenda at national and EU levels (first and the foremost the Horizon 2020 programme). NIS working group 3 (WG3) on "Secure ICT Research and Innovation" was primary responsible for this document, although the inputs from other WGs of the platform were taken into account.

The findings in this document have been obtained in various ways. NIS WG3 organised several expert meetings to structure its activities and prepare the main products in line with the objectives set out above. In particular, SRA brainstorming sessions were organised where WG3 members were asked to set out their visions of developments they hoped to see in the period to 2020.

The initial material produced was processed and three main areas of interest (AoIs) emerged, with the following titles:

1. Individuals' Digital Rights and Capabilities (Individual layer)
2. Resilient Digital Civilisation (Collective layer)
3. Trustworthy (Hyperconnected) Infrastructure (Infrastructure layer). This area is of particular interest and the following main infrastructures were identified:

- ICT Infrastructure
- Smart Grids
- Transportation
- Smart Buildings in Smart Cities
- Industrial Control Systems, including SCADA, in selected sectors (Water, Food/Agriculture, Nuclear, and Chemical Operation)
- Public Administration and Open Government
- Healthcare Sector
- Automotive / Electrical Vehicles
- Insurance

Each of the previous areas had a specific SRA, with short/mid/long terms research goals.

Eventually a cross-analysis have been performed and a positive property vision has been produced with the following areas:

2.3.2.2 ECSO and the Contractual Public Privacy Partnership in Cybersecurity

The European Cyber Security Organisation[30] (ECSO) was founded to underpin the contractual Public Privacy Partnership in Cybersecurity[31] (cPPP), in June 2016. The main goals of ECSO is to provide the support to the initiatives and projects on European Cybersecurity and, in particular, to

1. Foster and protect from cyber threats the growth of the European Digital Single Market (DSM);
2. Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry with an increased market position;

---

[28] 31st December, 2015, Strategic Research Agenda Final v0.96, https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/view

[29] http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm

[30] https://www.ecs-org.eu/

[31] https://www.ecs-org.eu/cppp

3. Develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.

The **Strategic Research and Innovation Agenda**[32] created by ECSO took as a basis also concepts and ideas from the NIS WG3 one. Although the main perspective was the market and technology one, when presenting the priorities. Still a significant presence of the vertical sectors and the splitting in security technologies, ICT technologies and cyber technologies and products is given.

In particular, ECSO SRIA v1.0 use the following classification for cybersecurity product and services (others could be used as well):

Cybersecurity Products & Services:

- Assurance, security / privacy by design
- Identity, access and trust management
  - Identity and access management
  - Trust management
- Data security
- Protecting the ICT Infrastructure and enabling secure execution:
  - Cyber threats management
  - Network security
  - System security
  - Cloud security
  - Trusted hardware/ end point security/ mobile security
- Cybersecurity services
  - Auditing, compliance and certification
  - Risk management
  - Cybersecurity operation
  - Security training

The "Products & Services" approach is a cornerstone of ECSO cPPP analysis for defining the technical priorities for the cPPP. In doing so ECSO will consider the vertical sectors (as smart grids, e-health,…) and their needs vs security products. The main goal is to provide a set of cybersecurity capabilities technologies that can be used in different application domains with maximum efficiency and impact.

In Figure 2 the vertical sectors (or application domains or hyper connected infrastructures as mentioned in the NIS WG3 SRA) with the products and eventually with the research areas/topics to be funded to fill the existing gaps.

The vertical sectors will provide requirements and needs to the lower layers, by requiring proper technologies and processed to secure the development and operation. These products in turn use security product and services.

Such vision in three main layers is also considered in the JRC taxonomy.

[32] 30th June, 2016, European Cybersecurity Strategic Research and Innovation Agenda for a contractual Public-Private-Partnership (cPPP). http://ecs-org.eu/documents/ecs-cppp-sria.pdf

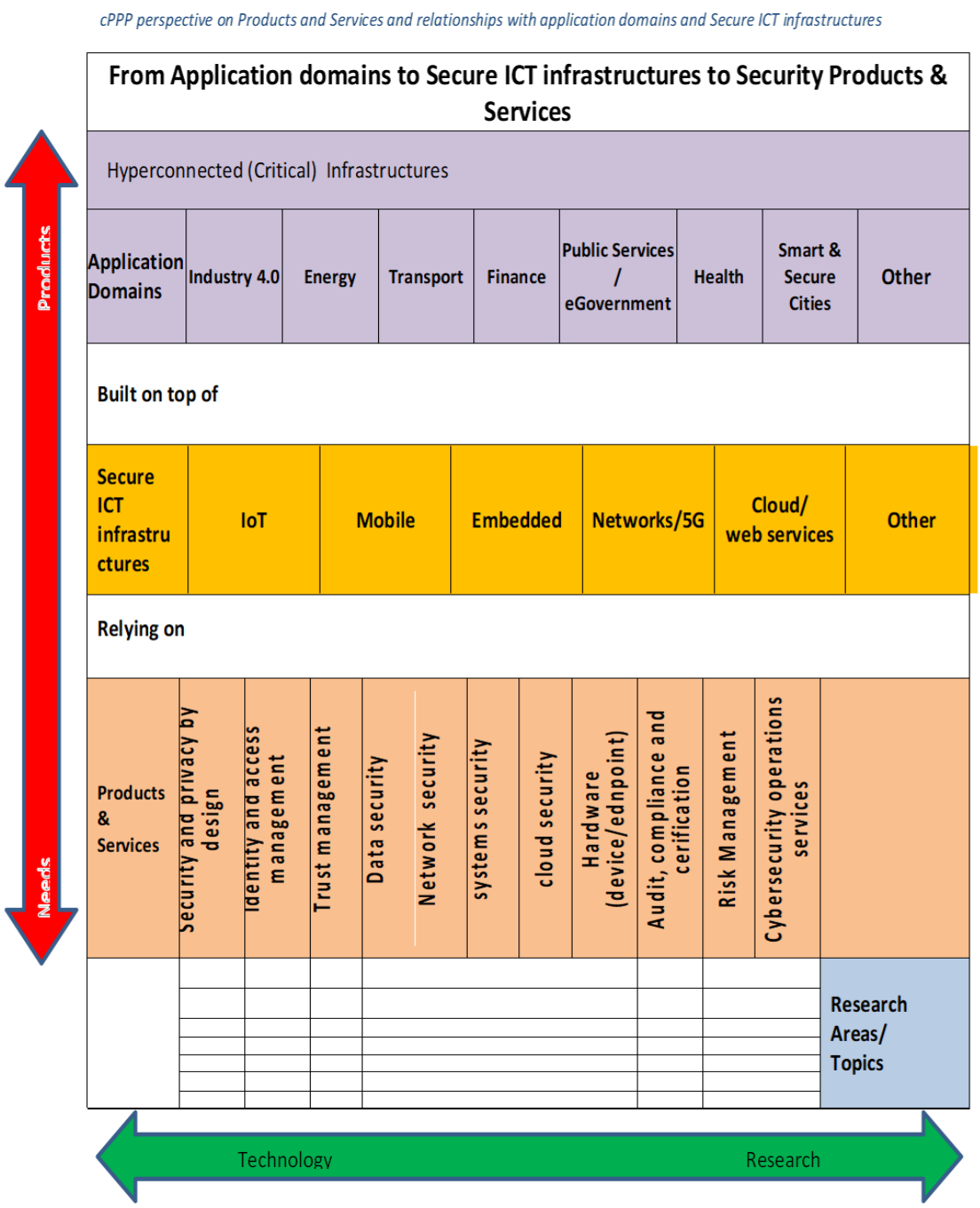


Figure 2: Structure of strategic research and innovation agenda of cPPP

2.3.2.3 ENISA

The European Union Agency for Network and Information Security[33] (ENISA) is positioning itself as a centre of expertise for cybersecurity in Europe. The agency releases an annual Threat Landscape report that provides a report about the most dangerous cyber threats in the past year and the changes in the global threat trends.

[33] https://www.enisa.europa.eu/

Also, the ENISA divided its activities in a number of topics[34]:

1. Cloud and Big data
2. Critical Infrastructures and Services
3. CSIRT Services
4. CSIRT and communities
5. CSIRT in Europe
6. Cyber Crisis Management
7. Cyber Exercises
8. Cyber Security Education
9. Data Protection
10. Incident Reporting
11. IoT and Smart Infrastructures
12. National Cyber Security Strategies
13. Standards and Certification
14. Threat and Risk Management
15. Training for Cyber Security Specialists
16. Trust Services

2.4 Results of the Desktop Analysis

We have aggregated the results from different sources by comparing the identified topics with the topics of our taxonomy. For every match we added a weighted (with respect to the significance of the document) value and normalised the results at the end. Table 2, Table 3, Table 4 provide the results of the desktop analysis.

Table 2: Mapping of EU and US cybersecurity technology topics

Cyber security technologies	US priorities	EU priorities
Security Management and Governance	0.79	1
Data Security and Privacy	0.53	0.73
Education and Training	0.47	1
Assurance, Audit, and Certification	0.16	1
Network and Distributed Systems	0.63	0.73
Identity and Access Management	0.79	0.35
Trust Management, Assurance, and Accountability	0.21	0.73
Human Aspects	0.63	0.38
Software and Hardware Security Engineering	0.79	0
Operational Incident Handling and Digital Forensics	0.63	0.27
Security Measurements	0.42	0
Cryptology (Cryptography and Cryptanalysis)	0.42	0
Legal Aspects	0	0
Theoretical Foundations	0.16	0

Security of a system is as strong as strong all its part, therefore it is very difficult to single out just a few areas which are the most important ones. From the analysis, we see *Security Management and Governance* gets "high" scores by both EU and US Nevertheless, the nature of our desktop analysis leaves the room for high dispersion and the following topics could be considered also highly relevant:

- Education and Training
- Network and Distributed System
- Data Security and Privacy
- Assurance, Audit and Certification
- Identity and Access Management

[34] https://www.enisa.europa.eu/topics

- Trust Management, Assurance, and Accountability
- Human Aspects

We also see some disproportion in some topics, such as *Assurance, Audit, and Certification* and *Trust Management, Assurance, and Accountability* which have high attention in EU and low in US, and *Software and Hardware Security Engineering* with the opposite scores.

Table 3: Mapping of US and EU priorities of ICT technology topics for cybersecurity

Applications	US priorities	EU priorities
Internet of Things	1	1
Cloud and Virtualization	0.42	1
Mobile Devices	0.37	1
Big Data	0.16	1
Operating Systems	0	0.73
Industrial Control Systems	0.21	0.38
Embedded Systems	0.74	0.35
Critical Infrastructures	0.63	0.35
Hardware	0	0
Supply Chain	0	0
Information Systems	0.37	0.35

We can easily see the technologies which require more progress in cybersecurity and privacy:

- Internet of Things
- Cloud Computing
- Mobile devices
- Embedded systems
- Critical Infrastructures

We should also underline the importance of *Big Data* and *Operating Systems* from the EU perspective as many of the analysed documents refer to these ICT technologies, while US does not pay explicit attention to this ICT technology. On the other hand, US devotes more attention to securing Embedded Systems and Critical Infrastructure.

Table 4: Mapping of US and EU priorities of application domains for cybersecurity

ICT Techonologies	US priorities	EU priorities
Energy	1	1
Public Safety	0.43	1
Transportation	0.43	1
Financial Services	0.43	0.73
Health	0	0.73
Nuclear	0.43	0.65
Telecom	0.43	0.65
Water	0.43	0.65
Supply Chain	1	0
Industry 4.0	0	0.73
Defense	0	0
Energy	1	1
Public Safety	0.43	1

The results of our analysis of applications for CSP are quite surprising, as many application domains which always required specific attention of CSP, such as *Healthcare and Industry 4.0* did not get much attention in US programmes. Probably,

this could be explained by the focus of funding agencies on critical infrastructure (as *Energy, Nuclear* and *Water* have got higher scores).

We can partially explain the lack of attention to such hot topic as security of *Transportation* in US by a clash of terms. From the analysis of ICT domains, we see that Embedded systems (which are used in Transportation) have got a lot of attention in US programmes, so do the Vehicular systems. Thus, the programme developers could simply avoid mentioning Transportation, as it could be seen as one of the most obvious application of Embedded or Vehicular systems.

Finally, low scores for *Defence* can be explained by the nature of selected documents for analysis. These documents are mostly related to general research programmes, while Defence is military driven and requires special attention. Moreover, we see that DoD and DARPA in US are the major funding agencies for CSP (see Section 2.3.1 Figure 1), while the specific programmes of DoD are not available for our analysis.

2.5 Survey Analysis

In May 2018, AEGIS carried out an online survey in the EU and the US to identify R&I priorities for future collaboration in cybersecurity and privacy as well as to pinpoint possible barriers to transatlantic cooperation.

The survey was conducted from 10 May 2018 until 31 May 2018. It was sent via email to ICT and cybersecurity researchers from academia and the industry, decision makers, government institutions and associations in the EU and the US. AEGIS used consortium partners´ well-vetted databases to select the recipients for the survey sample. In total, the survey was answered by 130 relevant stakeholders in the Cybersecurity and Privacy R&I and policy fields.

The results were presented in the Report on Cybersecurity and Privacy R&I Priorities for EU-US Cooperation[35].

Some category, sector and domains have different titles than those used in the AEGIS survey. This is because the survey used two taxonomies, the JRC and the NIST taxonomy, since it was meant to be answered by EU and US recipients.

The following section will summarize the survey results and focus on: respondent profiles; respondent participation and perspectives on cybersecurity research collaboration; cybersecurity research domain priorities; application and technology priorities; sector priorities; and perceived barriers for EU-US collaboration.

2.5.1 Respondent profiles

The survey provided valuable insight from individuals in the research sector and the private sector. Its biggest respondent groups were researchers (33,3%) and consultants (17,1%). In addition, researchers and professors together represented 48,4% of participants, while managers, directors and individuals in C-level positions made up 30,2%.

A majority of respondents declared that they worked at a university (33,3%) or a private company (31,0%). In terms of a geographical breakdown, 80,2% of survey participants were from the EU and 19,2% were from the US. Most respondents (70,7%) belonged to large entities, although 29,3% worked at small and medium sized organizations.

[35] https://drive.google.com/file/d/1o5F7TjuBYmfwC4PixjqfmJDM6WgQTNdi/view

2.5.2 Participation and perspectives on cybersecurity research collaboration

In order to assess interest in transatlantic cybersecurity and privacy research collaboration, participants were asked whether they had previous experience in such EU-US cooperative projects. 31,8% of respondents indicated that they had participated in transatlantic research projects.

Further data indicates that there is interest in participating in these collaborative R&I projects. 23,3% of participants said they were already planning to participate in EU-US cybersecurity research projects. Meanwhile, 65,1% said they would maybe participate in the future. Specific areas for collaboration mentioned in the survey cover cybersecurity and privacy related topics, including digital security, cybersecurity protection, cyber threat intelligence sharing, cybersecurity education, compliance, security engineering, Big Data analytics, governance of cybersecurity ecosystems, privacy, data governance, blockchain and cybersecurity testbeds.

The intention to participate in EU-US collaborative projects is relatively higher among US respondents. In the EU, 18.8% of survey participants said they were planning to participate in such projects. The result was 40,0% among US respondents. 67,9% of EU participants said they may take part in collaborative research projects in the future. On the same note, 56,0% of US respondents said they were planning to participate in the future.

In terms of the individual´s experience on collaborative EU-US research projects, most of the participants classified their experience as positive. 45,4% declared their experience had been "Positive" and 34,0% said their experience had been "Very Positive."

2.5.3 Cybersecurity research domain priorities

Survey respondents were asked to rate a separate list of 14 cybersecurity research domains, applications and technologies and sectors selected on the basis of the taxonomy described above in 2.2. Based on each subject´s importance for EU-US collaboration, participants used a scale of 1 – 4, where 1 was "Not Important" and 4 was "Very Important."

In terms of cybersecurity research domains, respondents indicated that Data Security and Privacy was a top priority, with a score of 3,75 and 80,8% of survey participants declaring it was very important. It was followed by Trust and Privacy (3,42) and the Fight Against Cybercrime (3,32), which were classified as very important by more than 50% of respondents.

Overall, all research domains received a score above average (2,5) and 11 of them were scored above 3 points, which indicates their significant relevance for transatlantic R&I cooperation.

Table 5: Survey results. Prioritised cybersecurity technologies for EU and US

Research Domains	Average	EU	US
Data Security and Privacy	3,75	**3,76**	**3,75**
Trust and Privacy	3,42	**3,47**	**3,29**
Fight Against Cybercrime	3,32	**3,42**	2,96
Cybersecurity Education	3,31	**3,37**	**3,17**
Compliance with Information Security, Privacy Policies and Regulations	3,24	3,32	3,00
Privacy Attitudes and Practices	3,16	3,19	**3,09**
Security Management and Governance	3,15	3,18	**3,13**
Security Engineering	3,13	3,13	3,08
Risk Management	3,06	3,08	3,00
Identity and Access Management	3,09	3,13	3,00
Information Security Behaviour	3,01	3,05	2,83
Security Measurements	2,99	3,01	2,92
Cryptology	2,82	2,87	2,67
Digital Forensics	2,79	2,87	2,54

2.5.4 Application and technology priorities

Participants declared that the most important application area was the Internet of Things. This area received a score of 3,64 and was ranked as very important by 71,3% of respondents. It was followed by Mobile Devices (3,56) and Big Data (3,48). These last two areas were ranked as very important for 61,9% and 57,9% of survey participants, respectively.

As with the research domain priorities, all application and technology areas were considered to be of considerable importance for cybersecurity research. All received a score above 3 points with the exception of Supply Chain, which was scored 2,98.

Table 6: Survey results. Prioritised ICT technologies for EU and US

Applications and Technologies	Average	EU	US
Internet of Things	3,64	**3,63**	**3,65**
Mobile Devices	3,56	**3,54**	**3,63**
Big Data	3,48	**3,48**	**3,50**
Cloud and Virtualization	3,50	**3,55**	**3,33**
Operating Systems	3,38	**3,42**	3,17
Industrial Control Systems	3,32	3,32	**3,30**
Hardware Technology	3,15	3,16	3,08
Supply Chain	2,98	2,96	3,08

2.5.5 Application domain priorities

Respondents overall gave importance to the six selected sectors. The Health domain, which received a score of 3,69, was considered the most relevant domain by 75,4% of survey participants. It was followed by the Financial Services domain (68,2%) and the Public Safety domain (64,0%).

In addition, the Transportation and Energy domains scored above 3 points. The Maritime domain, meanwhile, scored 2,95.

2.5.6 Perceived barriers for EU-US collaboration

Finally, the AEGIS survey asked participants to select the three main barriers facing cybersecurity and privacy R&I cooperation projects from a multiple-choice list.

Respondents indicated that the differences in policies and legislation on cybersecurity and privacy between the EU and the US was the primary barrier (71,2%). This was followed by the lack of coordination between funding programmes in both

jurisdictions (59,1%) and the fragmented cybersecurity field in the EU and the US (52,3%).

2.6 Overall Analysis

In this Section we aggregate the results of the desktop analysis and survey. We take the quantitative values received in the desktop analysis, the normalized (divided by 4, i.e., the maximal value) results of the survey and finding the average of the two. In case our survey did not use some topics, we leave the corresponding cells blank and propagate only the value of the desktop analysis. All the final tables are sorted by the total average value.

2.6.1 Cybersecurity Technology Topics

As shown in Table 7, the overall analysis of cybersecurity technology topics shows that *Security Management and Governance* is the most prioritised topic, closely followed by *Data Security and Privacy* and *Education and Training*. Then, we have five topics closely following one another.

It is easy to note that Cryptography gets a quite low score in both the EU and the US. In addition, *Legal Aspects* also has low values, regardless of the high score it received from the survey (here it was referred to "Fight Against Cybercrime").

Moreover, there are some mismatches among the priorities of the EU and the US. For example, the US has much higher scores for *Identity and Access Management* and *Software and Hardware Security Engineering* than the EU does. The opposite situation is seen for *Assurance, Audit and Certification* and *Trust Management, Assurance and Accountability,* where the EU scores are higher than the US scores. We see that the difference in the total scores is driven mostly by the values coming from the desktop analysis, while the results of the survey do not have such a significant difference.

Table 7: Total ranking for cybersecurity technology topics

Cybersecurity technology topics	Average			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Security Management and Governance	0.89	0.79	0.84	1	0.79	0.9	0.79	0.78	0.79
Data Security and Privacy	0.63	0.94	0.78	0.73	0.94	0.84	0.53	0.94	0.73
Education and Training	0.74	0.83	0.78	1	0.84	0.92	0.47	0.79	0.63
Assurance, Audit, and Certification	0.58	0.81	0.69	1	0.83	0.92	0.16	0.75	0.45
Network and Distributed Systems	0.68		0.68	0.73		0.73	0.63		0.63
Identity and Access Management	0.57	0.77	0.67	0.35	0.78	0.56	0.79	0.75	0.77
Trust Management, Assurance, and Acc.	0.47	0.86	0.66	0.73	0.93	0.83	0.21	0.82	0.52
Human Aspects	0.51	0.79	0.65	0.38	0.79	0.59	0.63	0.77	0.7
Software and Hardware Security	0.39	0.78	0.59	0	0.78	0.39	0.79	0.77	0.78
Operational Incident Handling and DF	0.45	0.7	0.57	0.27	0.71	0.49	0.63	0.64	0.63
Security Measurements	0.21	0.75	0.48	0	0.75	0.38	0.42	0.73	0.58
Cryptology	0.21	0.71	0.46	0	0.71	0.36	0.42	0.67	0.54
Legal Aspects	0	0.83	0.42	0	0.85	0.43	0	0.74	0.37
Theoretical Foundations	0.08		0.08	0		0	0.16		0.16

2.6.2 ICT Technology Topics

As shown in Table 8, *IoT* is the leader in our ranking of ICT Technology topics. However, for the EU, the difference between the first four positions is negligible. *Cloud and Virtualization, Mobile Devices* and *Big Data* go closely together after the leading topic. Meanwhile, *Operating Systems*, ranked number five, is quite behind.

We would like to note that *Embedded Systems* and *Critical Infrastructures* have very high scores in the US, but have low scores in the EU.

Table 8: Total ranking for ICT technology topics

ICT Technology topics	Average			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Internet of Things	1	0.91	0.96	1	0.91	0.95	1	0.91	0.96
Cloud and Virtualization	0.71	0.88	0.79	1	0.89	0.94	0.42	0.83	0.63
Mobile Devices	0.68	0.89	0.79	1	0.88	0.94	0.37	0.91	0.64
Big Data	0.58	0.87	0.72	1	0.87	0.94	0.16	0.88	0.52
Operating Systems	0.37	0.85	0.61	0.73	0.85	0.79	0	0.79	0.4
Industrial Control Systems	0.3	0.83	0.56	0.38	0.83	0.61	0.21	0.83	0.52
Embedded Systems	0.54		0.54	0.35		0.35	0.74		0.73
Critical Infrastructures	0.49		0.49	0.35		0.35	0.63		0.63
Hardware	0	0.79	0.39	0	0.79	0.4	0	0.77	0.39
Supply Chain	0	0.75	0.37	0	0.74	0.37	0	0.77	0.39
Information Systems	0.36		0.36	0.35		0.35	0.37		0.37
Vehicular Systems	0.26		0.26	0		0	0.53		0.53
Pervasive Systems	0		0	0		0	0		0

2.6.3 Applications

As shown is Table 9*, Energy* is considered the most important area in terms of Applications. It is followed by *Public Safety* and *Transportation*. Moreover, we would like to point out the low score received by the *Transportation* application in the US. It could be inferred that *Transportation* got a low score because it might be considered a part of *Embedded Systems* (ICT Technology, with very high score for the US). *Public Safety, Financial Services* and *Healthcare* also have low scores in the US (especially for the desktop analysis). Finally, we see that *Supply Chain* obtains a maximum score in the US and a minimal score in the EU. This topic was not investigated in our survey and we cannot confirm the findings.

Table 9: Total ranking for applications

Application domains	AVG			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Energy	1	0.85	0.92	1	0.86	0.93	1	0.8	0.9
Public Safety	0.71	0.89	0.8	1	0.91	0.95	0.43	0.81	0.62
Transportation	0.71	0.86	0.78	1	0.86	0.93	0.43	0.85	0.64
Financial Services	0.58	0.9	0.74	0.73	0.91	0.82	0.43	0.87	0.65
Health	0.37	0.92	0.64	0.73	0.92	0.83	0	0.93	0.46
Nuclear	0.54		0.54	0.65		0.65	0.43		0.43
Telecom	0.54		0.54	0.65		0.65	0.43		0.43
Water	0.54		0.54	0.65		0.65	0.43		0.43
Supply Chain	0.5		0.5	0		0	1		1
Industry 4.0	0.37		0.37	0.73		0.73	0		0
Defense	0		0	0		0	0		0

3 CRITICAL APPLICATION DOMAINS AND DEMAND FOR CYBERSECURITY AND PRIVACY

AEGIS has selected several application domains for analysis in order to determine whether the prioritised cybersecurity technology topics adequately address the real needs of the selected application domains. Our analysis has primary focused on the following three domains – Maritime, Healthcare and Financial – for various reasons. The need for cybersecurity and privacy in the Healthcare and Financial applications has long been acknowledged by various initiatives and projects. Recently, the Maritime domain has gained more and more attention (e.g., see the latest US National Cybersecurity Strategy) since it has a great number of CSP challenges that need to be solved.

For the analysis of the coverage of the needs of every application domain by R&I funding programs, we specified the importance of every cybersecurity technology topic for every application and compared it with the results of our overall analysis (see Table 7). By comparing these values, we are able to identify the areas of high (and/or medium) importance which received more (or less) attention than required.

Naturally, such analysis is limited to the amount of selected application domains (we have chosen to analyse only three out of many other potential applications requiring improvement from the CSP point of view). The results of the analysis are also affected by AEGIS project partners, since the classification of the importance of these topics depends highly on our experience. On the other hand, AEGIS partners are experienced researchers in CSP and took an active part in defining priorities for CSP at national and international levels.

3.1 Maritime

In terms of the civilian aspect of this domain, we consider Maritime a subdomain of transportation and storage. Researchers have identified significant weaknesses in the critical technology used for navigation at sea.

The general concern for this domain is that infrastructure and transportation are not up-to-date in terms of security protection. The lifetime of a modern vessel is about 25-30 years, but there are a lot of non-modern vessels out there over 30 years old that are often not updated with the latest technologies. Additionally, they often have devices with poor security.

Cybersecurity protection must be increased with new IoT technology on modern leisure cruisers to help identifying passengers and to protect the IT on board. The GPS system is one of the weakest elements of the transportation domain. If the GPS System is compromised, there is potential for serious consequences.

For example, there are serious potential consequences if cyber attacks target the container tracking software used by ports or navigation systems. There is a risk to life and property if such attacks cause vessel collisions. Even without collisions, systematic delays would cause finance and transportation issues, which in turn could create an impact worldwide on commerce activities. Likewise, attacker threat groups specialised in business email compromise (BEC) and business email spoofing (BES) fraud target maritime shipping firms resulting in millions of dollars stolen on an annual basis.

This domain as very large surface cyber attack. According to our analysis of cyber threats occurred in 2018 (up to the end of August): 14 Identified attack over Transportation domains (that are disclosed):

Table 10: Distribution of attacks for Transportation domain

Type of Attack	%
Unknown	42.9%
Account Hijacking	21.4%
Defacement	14.3%
DDoS	14.3%
Targeted Attack	7.1%

3.2 Healthcare

The Healthcare domain includes several sectors that provide goods and services to treat patients. This domain includes, for example, hospitals, medical device manufacturers and the pharmaceutical industry. There are increased possibilities for cyber attacks in this domain area because many elements are interconnected.

There are also possibilities of cyber attacks in the Healthcare domain when it comes to IoT "Medical Devices." The IoT Medical Devices are "cloud-connected" via Bluetooth or RFID/NFC, a vulnerability identified by the researchers and published in the NIST/CV. If these devices were to come under attack, the perpetrators could falsify or deactivate the data, and/or modify the release of medicine.

Nowadays, healthcare is moving out of the hospital and into the patient's home. From home, it is then possible to connect to a hospital network and connect to devices to share data with medical staff. Key stakeholders in the Healthcare domain, including device vendors, need to think proactively about how to keep their devices and their patients' lives safe while not compromising clinical functionality.

This domain is very exposed to cyberattack, according to our analysis of cyber threats occurred in 2018 (up to the end of August): 61 Identified attack over Human health activities (that are disclosed):

Table 11: Distribution of attacks for Healthcare domain

Type of Attack	%
Malware	39.3%
Account Hijacking	34.4%
Unknown	21.3%
Targeted Attack	3.3%
Credential Stuffing	1.6%

3.3 Financial

The financial domain is very appealing for cyber attackers mainly because of the money at stake. Additionally, the liquid market of cryptocurrency is also attractive to criminals.

For example, criminals are now using "fake news" to carry out lateral attacks in the finance domain. In one case in the EU, activists published fake news that caused 15 minutes of panic in the stock market and provoked a vast loss of money.

Another aspect in the Financial domain that must be considered is the user. When it comes to products such as online banking and other financial services, the user is alone and must protect himself. This could cause consequences in other areas of the financial domain. For example, malware installed in a user´s device, besides causing problems for the user, could penetrate the financial service´s network.

This domain is very exposed cyberattack according to our analysis of cyber threats occurred in 2018 (up to the end of August): 47 Identified attack over Financial and insurance activities (that are disclosed):

Table 12: Distribution of attacks for Financial domain

Type of Attack	%
Malware	29.8%
Unknown	27.7%
Targeted Attack	14.9%
DDOS	12.8%
Account Hijacking	12.8%
Fraudulent SWIFT	2.1%

3.4 ICT Technology Analysis Summary

For the analysis of the coverage of the R&I funding needs in the three focus domains, we specified the importance of every cybersecurity technology topics and compared it with the results of our overall analysis (Table 7) in Table 13.

Table 13: Comparison of R&I priorities in the US and the EU for the three focus domains

CSP technologies	Maritime	Health	Financial	EU priority	US priority
Assurance, Audit, and Certification	High	Medium	Medium	0.92	0.45
Cryptology (Cryptography and Cryptanalysis)	Medium	Medium	High	0.36	0.54
Data Security and Privacy	High	High	High	0.84	0.73
Education and Training	High	High	Medium	0.92	0.63
Operational Incident Handling and Digital Forensics	Medium	Low	High	0.49	0.63
Human Aspects	High	Medium	High	0.59	0.70
Identity and Access Management (IAM)	High	High	High	0.56	0.77
Security Management and Governance	High	Medium	High	0.90	0.79
Network and Distributed Systems	Medium	Medium	High	0.73	0.63
Software and Hardware Security Engineering	Medium	High	Medium	0.39	0.78
Security Measurements	Medium	Medium	High	0.38	0.58
Legal Aspects	Low	Medium	Medium	0.43	0.37
Theoretical Foundations	Low	Low	Medium	0.00	0.16
Trust Management, Assurance, and Accountability	High	Medium	High	0.83	0.52

Our reasoning behind the importance rating is as follows. *Assurance, Audit and Certification* is high for Maritime, as this domain is very heterogeneous (and dynamic) and many sub-systems (ships, ports, containers, coast guards, etc.), which belong to different stakeholders (and even countries), communicate. On the other hand, in contrast to Health and Financial domains, Maritime has got little attention from cybersecurity so far.

Cryptology is high for Financial domain as secrecy of transactions has to be maintained. *Data Security and Privacy* has high importance for all domains, since they all store, transmit and manage third party data. *Education and Training* is put to medium for Financial domain as the importance of cybersecurity in it is long

recognized and much more attention has been devoted to education and training in this domain already.

Operational Incident Handling and Digital Forensics is high for Financial domains, as it is important for tracing the cyber criminals; while we put low importance for Health domain, since although prosecution of criminals in this case is required as well, it is difficult to mitigate the further harm the attackers can do after the attack.

Human aspects are high for Maritime and Financial domains as they are more susceptible for phishing attacks. *Identity and Access Management* is high for all domains, as rightful access to data is important.

Security Management and Governance is particularly challenging for Maritime domain as it is very heterogeneous and has no well-known dedicated guidelines for cybersecurity risk management; Financial domain still needs advancement in this direction as economic impact of cyber risks seriously impact the overall enterprise governance.

Network and Distributed Systems has high rating, since businesses now much depend on IT, and often depend on the external IT provider (e.g., cloud), which raises the complexity of network management and makes business (and the "system") more distributed.

Software and Hardware Security Engineering is a bit higher for Healthcare as with more reliance on IT the attacker receive more ways to impact people (patients) by compromising devices.

Financial domain requires *Security Measurements* more than others, to balance losses and benefits more precisely (e.g., cyber insurance or banking sector).

Legal aspects are considered of low importance for Maritime domain, mostly because currently cybersecurity for this domain is not well developed and this issue yet to come to play for the domain later.

Theoretical foundations are important per se and are a useful basis for the future innovations, but in many domains, such as Maritime or Health, the urgent problem is to implement the existing cyber security techniques rather than to introduce conceptually new approaches.

Finally, *Trust Management, Assurance, and Accountability* can be seen slightly higher for Maritime and Financial domains, as they are more heterogeneous and require interaction of systems which belong to various stakeholders (and even countries).

In our ICT technology analysis, we determined that in the majority of cases, the most important cybersecurity technologies are well covered by existing R&I programmes. There are only a few topics that require specific attention.

First, we would like to underline the striking difference between the moderately high demand for *Cryptography* in many application domains and lack of attention paid to this area by R&I programmes in both the EU and the US. A possible explanation for this mismatch could be the fact that many ICT technologies and application domains simply require suitable methods for the application of cryptography, rather than new and stronger cryptographic schemas. Nevertheless, the topic itself should not be ignored, especially with the development of quantum cryptography.

Secondly, we see that *Assurance, Audit and Certification* is considered a topic of moderate importance. While it is considered a high priority area in the EU, it is not well covered in the US. This is an area where the EU could share its expertise with the US, as many ICT technologies require strong evidence of compliance with various standards and legislations. A similar situation can be observed with *Trust Management, Assurance and Accountability* topic.

On the contrary, *Software and Hardware Security Engineering* receives little attention in the EU but is considered high priority in the US. The importance of the topic for various application domains means it cannot be overlooked. The EU could explore this ICT technology topic more to obtain the required knowledge in collaboration with the US. Similarly, we see only moderate attention in EU to such hot topic as *Identity and Access Management*

Finally, *Legal Aspects* did not get much attention in the EU or in the US, although it has been found to be moderately important for many ICT technology topics. The lack of attention can be partially explained by the perception that this aspect should be dealt with by legal research programmes. Although this may be true, technical support and vision is required for the correct formulation and enforcement of cybersecurity laws.

4 RECOMMENDATIONS FOR US-EU COLLABORATION FROM DIFFERENT PROJECTS

This section highlights a number of recommendations from past EU-US cooperation projects in cybersecurity and privacy.

4.1 FP7 Inco-Trust and BIC Projects

The first officially EC funded EU-US cooperation project for cybersecurity and privacy was entitled INCO-TRUST (long name: International Co-operation in Trustworthy, Secure and Dependable ICT infrastructures). INCO-TRUST ran from 1st January, 2008 until 31st December, 2010 under the portfolio of Unit 'F5', ICT Trust and Security.

The main purpose of the INCO-TRUST CA, specifically targeting international cooperation in the area of Trustworthy, Secure and Dependable ICT infrastructures, was:

1. To promote collaboration and partnerships between researchers from the developed countries (EU, US, Japan, Canada, Australia, Korea) with the goal of coordinating the multiple research efforts underway in the areas of ICT Trust, Security and Dependability (TSD).
2. To leverage and harmonise efforts on the respective sides related to the building and maintenance of large-scale trustworthy ICT systems and infrastructures and the services they deliver.

Within the final deliverable of the project, **D3.1 The INCO-Trust Recommendations report**, the project analysed the EU – US cooperation situation and identified two groups of recommendations that are labelled under the categories *Strategic* and *Tactical*. The project recommendations were road mapped for future FP7/FP8 calls in the report for both groups of recommendations. The following contains a listing of the INCO-TRUST recommendations.

(a) ***Strategic* Recommendations** (SRs): On a more **strategic** level, the EU – US ICT trust and security communities should collaborate on the following:

SR1 ***International alignment***: preparation of policy frameworks to enable global collaboration and interoperability;

SR2 ***Variety***: cooperation on topics related to security and diversity;

SR3 ***Scalability***: cooperation on topics related to security and complexity;

SR4 ***Reciprocity***: cooperation on topics related to security and interoperability;

SR5 ***Secrecy***: cooperation on the issues of digital sovereignty and dignity;

SR6 ***Negotiation****:* cooperation on the theme of security and trust;

SR7 ***Security expertise***: cooperation on topics related to security and technological challenges of security;

SR8 ***Protection***: cooperation on topics related to security and cyber-defence.

(b) ***Tactical*** Recommendations (TRs)***:*** The international ICT trust and security community should **tactically** collaborate on research to:

TR1 Support **strengthening infrastructure resilience** and control crisis management;

TR2 Support **securing the current and future internet** related to diversity, complexity and interoperability;

TR3 Support **securing cloud computing** for enterprises;

TR4 Support designing **identity and accountability management frameworks**;

TR5 Support new **privacy infrastructure**, reconsidering privacy spaces, storage function areas;

TR6 Support **repositioning trust infrastructure** at the same level as security infrastructure;

TR7 Support **metrics and standardization** issues;

TR8 Initiate **green** security;

TR9 Support cooperation in **cyber-defence** against the asymmetric challenge;

TR10 Enable the **engineering** of **secure and trustworthy software and systems**.

4.2 H2020 DISCOVERY

The next project dealing with EU – US cooperation was the DISCOVERY project (long name: Dialogues on ICT to Support COoperation Ventures and Europe-North AmeRica (Canada and USA) sYnergies). DISCOVERY was funded in Horizon 2020 under grant number 687780 within the ICT International cooperation portfolio of projects. Even though DISCOVERY was looking at cooperation between EU and US on a number of different ICT domains, there was a dedicated Working Group focussing on cybersecurity within the project's Transatlantic ICT Forum.

The DISCOVERY project made a number of focussed recommendations for specific domains, including Enterprises, Government, IoT research and industry. The most relevant recommendations of the project for this deliverable are listed below.

4.2.1 Recommendations for Governments

The recommendations for governments underline that security does not reside in Compliance but in an in-depth defense and an understanding of the risks related to lack of personnel and understanding about new technologies.

- It is necessary to take an International Approach to Cyberspace.
- The necessity of a secure E-government.
- Solidify Information Sharing Strategy in terms of cybersecurity.
- Invest in Cyber security.
- Invest in Cyber Education and Training.
- Maintain Voluntary Engagement on Securing Critical Infrastructure.

4.2.2 General Recommendations

Key recommendations of relevance to the EU – North America cooperation in the Cybersecurity and privacy fields include the following:

- Security automation
- Dynamic Security
- Advanced security approaches
- Mobile security

4.2.3 International Project Ideas

In addition to recommendations on research and innovation areas to consider for cooperation, a number of concrete **potential project ideas** were recommended during the DISCOVERY and other related events.

Establishment of close collaborations and collective visions and strategies for cybersecurity related Public-Private-Partnerships (PPPs) on both sides of the Atlantic. Although there are many policy and regulatory efforts establishing PPPs in both

Europe and the US, the results of these activities have been mixed and have only had a focus on their own jurisdictions activities.

The development of a project in relation to "cybersecurity ethics." While the privacy community has made significant progress in the ethical understanding of privacy and data use, there is still no corollary for the cybersecurity community and this issue needs to be urgently addressed.

The impact of the EU's GDPR on the development of IoT based systems and devices. Taking this a step further, it should also be examined in more detail how the proposed Regulation on Privacy and Electronic Communications[36] to replace the 2009 ePrivacy Directive will align in practice with the rules for electronic communications services within the EU's GDPR[37], especially in relation to IoT based systems and devices.

A project idea related to the cybersecurity of robots and connected, acting objects (actuators), in terms of sovereignty and dignity, from the users' point of view. It should incorporate issues of responsibility of autonomous cars, of accountability for the actions of reacting IoT systems, of consequences of chained communications of various connected objects, acting in community and freedom, which will soon present challenges that go beyond the strict legal responsibility of automata and software, in general.

4.3 H2020 PICASSO Project

The PICASSO project[38] was another H2020 funded project focussed on EU – US cooperation, specifically in ICT Policy, Research and Innovation for a Smart Society: Towards New Avenues In EU-US ICT Collaboration.

As part of their transatlantic events, there were a number of panel sessions dealing with cybersecurity and privacy and the AEGIS partners took part in these expert panels, providing inputs to their recommendations and reports.

One panel focussed on how developed solutions must enable the desired services and applications, whilst **respecting the EU and US privacy and data protection frameworks**. The difficulties of harmonising the EU's GDPR in the US were highlighted and some ideas about coming up with an incentive scheme that would help with companies to adopt the GDPR in other countries e.g. US, which would enable them to attract a larger EU-based market.

It was stressed that an excellent topic for EU – US collaboration would be on **cyber ethics**, which had already been suggested in the H2020 DISCOVERY project's Cybersecurity Working Group, and backed up at a recent forum of the UK/US summit and this topic should clearly be addressed from the EU/US perspective.

The panel focus then shifted to cybersecurity, and the panellists focussed on two approaches for EU - US collaboration on cybersecurity.

1. **Awareness raising of vulnerability issues** and ensuring stakeholders take their responsibility in the whole ecosystem;
2. **System wide redesign of computing and communications systems** we increasingly rely on.

---

36 https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

37 https://ec.europa.eu/digital-single-market/en/online-privacy

38 http://www.picasso-project.eu/

4.4 H2020 (Marie Curie) PROTASIS Project

The PROTASIS: Connecting the dots ... project is a Marie Sklodowska-Curie Research and Innovation Staff Exchange (RISE) project, whose aim was to extend the reach of the EU based Systems Security (SysSec[39]) community to the international community, including the United States. PROTASIS's goal is to set up a joint research programme in the area of Systems Security spearheaded by the need to develop a computing infrastructure that will be trusted by the citizens and the organizations they use it. Through a novel international and inter-sectoral programme, the participants aim is to advance the state-of-the art in the area of security and privacy and will sharpen their skills using the most advanced methods for cyberattacks and malware.

SysSec and PROTASIS partners have identified a few grand challenge problems and they feel that solving them will be a major step towards creating a trusted and safe cyberspace. These **Grand Challenges** include:

- **No Device Should Be Compromisable:** Develop the necessary hardware and software support to make it impossible for attackers to compromise a computer or communication device for that matter, including smartphones and tablets.
- **Provide Private Moments in Public Places:** Enable users to have private communication in the public areas of the cyberspace.
- **Give Users Control Over Their Data**: Provide the necessary mechanisms so that users:

1. will be able to know *which data they have created* (such as text, photos, videos, cookies, web requests, etc.);
2. will be able to know *what data they have given to third parties* (such as text, photos, cookies, web requests, IP addresses, etc.);
3. will have the *capability to refuse disclosure of some data* (such as cookies and IP addresses) and still expect a decent level of service;
4. will have the *capability to delete their own data which they have created* (both from the local storage as well as from the cloud);
5. will, under an appropriate legal framework, *have the ability to ask past recipients of their data to erase them as well.*

Develop Compromise-Tolerant Systems: Provide adequate security levels even if components of the system have been compromised.

[39] http://www.syssec-project.eu/

5 AEGIS RECOMMENDATIONS FOR EU-US COLLABORATION IN CYBERSECURITY AND PRIVACY R&I

Today, it is widely accepted that international cooperation is needed to address modern cybersecurity and privacy challenges. Sustained and coordinated investment in R&I should advance various areas of cybersecurity and arm the industry and public with advanced and efficient techniques to prevent cybercrimes.

5.1 Recommendation 1: Areas for Collaboration

Cybersecurity Technologies

Our analysis shows that many cybersecurity technologies have high level of importance. These technologies are highlighted in funding strategies and from the point of view of specific researchers. This can be explained by the nature of cybersecurity, which requires the safeguarding of all possible aspects in order to guarantee protection for data, processes and people. Failure in one aspect means failure of the whole protection system. Thus, a short (non-exhaustive) list of possible topics for R&I collaboration topics includes:

- *Security Management and Governance;*
- *Data Security and Privacy;*
- *Education and Training;*
- *Assurance, Audit, and Certification;* and
- *Network and Distributed Systems.*

ICT Technologies

Our analysis indicates that the following ICT technologies attract a lot of attention from both funding programmes and researchers:

- *Internet of Things;*
- *Cloud and Virtualization;*
- *Mobile Devices;*
- *Big Data;* and
- *Operating Systems.*

These are the ICT technologies that require more progress from the CSP point of view and appear to be promising in the EU and the US. With this in mind, these technologies are the most attractive for R&I collaboration projects.

Applications

The following applications require more progress with respect to CSP:

- *Energy;*
- *Public Safety;*
- *Transportation;*
- *Financial Services;* and
- *Health.*

5.1.1 Implementation Suggestions

Funding programme managers: Develop specific programmes within usual CSP R&I funding programmes (or as cross-programme collaborative projects) on the topics listed above.

5.1.2 Expected Impact

- Announcement and execution of special calls for international projects;
- Creation of EU-US international projects;
- Knowledge exchange between the EU and the US on the specified topics; and
- Strengthened relationships between R&I entities across the Atlantic.

5.2 Recommendation 2: Take an International Approach to Cybersecurity

The cyber world cannot be easily fragmented into national segments. It is global. This is understood by the businesses as well as by cyber criminals, who exploit cross border obstacles to get away with their crimes. Governments should do what is necessary to develop and encourage collaborative R&I projects in order to fight cybercrime on the global level, develop new cross-border cybersecurity policies and contribute to international cybersecurity standards. The experience gained applying available tools, such as the NIST Framework in the US or the General Data Protection Regulation (GDPR) in Europe, should be shared and promoted globally.

5.2.1 Implementation Suggestions

Government: Increase efforts to counter cross-border cybercrime.

Funding programme managers: Establish cross-programme calls for R&I projects on countering international cybercrime.

5.2.2 Expected impact

- Increase in international projects on fighting cross-border cybercrime;
- Knowledge exchange and growth due to collaboration;
- Increased collaboration between crime fighting agencies in the EU and the US; and
- Reduced number of cybercrimes, as the result of the futility of hiding behind borders.

5.3 Recommendation 3: Invest in International Cybersecurity Projects

Although ICT technologies quickly penetrate our lives and economy (cars, smart houses, industry 4.0, etc.), we under invest in cybersecurity. The high rate of evolving technologies leaves us unprotected when facing criminals that adapt quickly. It is important to note that the dark cyber world presents a unified front against fragmented national forces. We should aim at uniting our research and development teams and exchanging knowledge if we do not want to lose this fight.

5.3.1 Implementation Suggestions

Funding programme managers: Redirect or allocate money for international CSP R&I projects.

Government: Increase funding for cybersecurity.

5.3.2 Expected Impact

- Increased interest in international CSP collaboration;
- Increased knowledge exchanges and experience sharing in the field of CSP;
- Strengthened relations between R&I entities across the Atlantic; and
- Development of new schemes for fighting cybercrime on inter-organisational and international levels.

5.4 Recommendation 4: Establish or Improve International Coordination Between Funding Programmes

Every research and innovation funding programme has its own goals. The primary focus of these programmes is on generating benefits for the funding nation (or union). However, true international collaboration (between the EU and the US, in this case) should aim for mutual benefit. It is fair when beneficiaries gain funds proportionate to their contribution and are treated as equal partners rather than supporters. In order to truly achieve this for cross-border collaborations, there is a need for improved collaboration between funding programmes in order to ensure there are benefits for their respective nations. This is also required to ensure the programmes are providing the required resources.

5.4.1 Implementation Suggestions

Funding programme managers: Find and establish contacts with cross-Atlantic funding agencies. Organise collaborative programmes. Specify common goals, funding procedures and rules for collaboration.

5.4.2 Expected Impact

- Establishment of collaborations between different funding programmes;
- Exchange of best practices for running funding programmes;
- Announcement and execution of special calls for international;
- Creation of EU-US international projects;
- Knowledge exchange between the EU and the US on the specified topics; and
- Strengthened relationships between R&I entities across the Atlantic.

It should be noted that there are already some interesting EU–US collaboration programmes underway using a joint programme (with separate funding by each country) approach. As an example, lessons could be learned from the pairing of the EC DG CONNECT Next Generation Internet (NGI[40]) programme with the US National Science Foundation´s US-EU Internet Core & Edge Technologies (ICE-T[41]) initiative.

5.5 Recommendation 5: Reduce Legislation Barriers for Collaboration on Cybersecurity and Privacy

Differences in policies and legislations on CSP between the EU and the US is one of the main obstacles for R&I cooperation[42]. This obstacle arises from the different ways of treating third party data, often required for a comprehensive analysis, as well as from the protection of the intellectual rights that apply to the results of collaborative R&I projects. Harmonizing legislative frameworks is required to ensure that the information processing mechanisms for all involved parties are aligned and that know-how is protected.

5.5.1 Implementation Suggestions

Policy makers: Harmonize legislation requirement frameworks. Develop special cases for the research use of data to reduce unnecessary burdens for researchers.

Funding programme managers: Cooperate with other research funding programmes from other countries to establish basic rules for legal issues in international projects. Develop a simple framework template to deal with major legal

[40] http://www.ngi.eu/

[41] https://www.nsf.gov/pubs/2018/nsf18535/nsf18535.htm

[42] D.1.3 - White Paper on Cybersecurity Policies includes a comparative analysis between US and EU cybersecurity policies.

issues (e.g., data treatment) which ensures fulfilment of legal requirements in the EU and the US and can be applied in most of research projects. Some important special cases also should be considered. The procedure for solving any legal issue beyond the project should be provided to the researchers involved in collaborative projects.

5.5.2 Expected Impact

- Establishment of relaxed legal approaches for collaborative;
- Increased number of collaborative research project; and
- Researchers feel more confident about legislative procedure and devote more attention to their research.

5.6 Recommendation 6: Promote Information Sharing for Cybersecurity

The increasingly changing dynamics of the cyber world require rapid adaptation to ever changing conditions. This statement is especially true with respect to cybersecurity, where a situation could change in a matter of days from normal to dangerous, as we saw with the WannaCry outbreak in 2017. Therefore, timely sharing of threat information is a necessary to develop a solid strategy and protect against up and coming threats. The available information exchange mechanisms should be improved. Moreover, the data analysis needs to become more efficient while preserving the privacy of the participants.

In addition, besides promoting collaboration in information sharing, there is also a need to encourage entities to share their data for the mutual benefit of society. This is the area where cyber criminals are more effective than the law-abiding society.

5.6.1 Implementation Suggestions

Government: Encourage information sharing between governmental agencies at national and international levels. Provide researchers access to this data.

Funding programme managers: Support research of information sharing schemas, especially ones guaranteeing security and privacy.

5.6.2 Expected Impact

- Increase in information sharing activities and data pools available for analysis;
- Boost in CSP R&I as a result of the availability of data;
- More effective CSP solutions and assessment methods;
- Better understanding of security solution effects and attacker behaviour; and
- Faster and more effective reactions on emerging cyber threats.

5.7 Recommendation 7: Cyber Education and Training

The next generations will live in a much more digitized world and they will inevitably face even higher cybersecurity challenges than we do. Therefore, they have to be properly educated to meet these challenges. Naturally, governments must invest more in education and training programmes (some good examples of such programmes were highlighted during the Transatlantic ICT Forum in November 2016) to produce enough cybersecurity experts to satisfy the growing demand for these specialists.

In addition to experts, governments will have to raise cybersecurity awareness among ordinary citizens. These citizens will not work in cybersecurity but still must understand cyber risks and the simple, yet important, security practices that should be applied as well as their role in global cyber protection. Considering that cybersecurity education is a new (but highly demanded) discipline, international

cooperation and experience exchange is the key to building efficient training programmes and creating a more cybersecurity aware society.

5.7.1 Implementation Suggestions

Funding programmes managers: Devote more attention to projects that provide innovative methods for cybersecurity education and awareness raising. Support international cybersecurity training and awareness event participation.

Government: Create special collaboration programmes for cyber education and training similar to the Marie Curie Actions for the exchange of PhD students.

5.7.2 Expected Impact

- Increased number of international events with foreign participants and lecturers;
- Promotion of better coordination and awareness raising of the best practices of the existing initiatives related to cyber education and training;
- Increased exchange of experience, techniques and tools for cybersecurity education, training and awareness; and
- Elevated level of education in both jurisdictions.

5.8 Recommendation 8: Support Securing Critical Infrastructure

Critical Infrastructure in general used to be separated as much as possible from the common networks, but the advantages of being interconnected have started to shadow the drawbacks. This provides attackers with the opportunity to cause physical damage, which could have potentially catastrophic effects.

These possibilities attract very serious attackers, such as national security agencies and terrorists, who may have extensive security knowledge, powerful tools and vast resources, making protection of Critical Infrastructures even more challenging. The importance and difficulty of this task requires mobilising various resources, timely knowledge sharing and international (as well as national) support.

5.8.1 Implementation Suggestions

Funding programmes managers: Establish programmes for collaborative projects in specified fields (Energy, Water, Nuclear, etc.) and encourage the information sharing in these domains.

5.8.2 Expected Impact

- Increased number of international projects on secure Critical Infrastructure;
- Increased knowledge exchange and growth due to collaboration;
- Increased relations between crime fighting agencies in the EU and the US; and
- Increased number of solutions for various Critical Infrastructures.

5.9 Expert analysis of AEGIS recommendations

AEGIS conducted 20 in-depth interviews in Europe and the US with leading cyber security researchers and key stakeholders from the industry, in order to gather insights on the EU/US landscape on cybersecurity and privacy and on the AEGIS recommendations for transatlantic R&I cooperation. The guidelines for the interviews are included in Annex 2. Although the experts interviewed have different perspectives, in general, they share the views of AEGIS. Their insights are summarised in the following sections.

5.10 Cyber security technologies

With respect to the Cyber security technologies, the experts have mostly agreed with our proposal. Several of them underlined the importance of economic approaches for

cyber security management (e.g., risk management). Among the additional topics proposed by the experts we are able to single out only *Operational Security* (i.e., *Operational Incident Handling and Digital Forensics* in our taxonomy), which were mentioned by 2 participants.

5.10.1 ICT technologies

Although there was no much critics of our proposals, many experts highlighted two additional (and novel) topics which will require attention of cyber security in the nearest future: Artificial Intelligence (Machine Learning) and Blockchain.

5.10.2 Application domains

For application domain recommendations, we have also got mostly positive feedbacks. *Public Safety* has received a bit controversial assessment by the participants: some of them proposed to substitute the domain with another one, while the others marked it as the most important domains to focus on. As for other additional domains, there was no notable agreement among experts.

5.10.3 Recommendations

All recommendations we proposed were found useful. Additionally, the experts proposed their recommendations. We see that many of them target foster the dialog between EU and US or to raise the level of knowledge in cyber security. Many of these proposals are concrete actions and contribute well to our proposed implementation suggestions.

Fostering dialogue for collaboration (mostly contributing to our Recommendation 4):

- Organise a joint dissemination event;
- More opportunities for face-to-face interactions;
- Increase the number of visas for third country technical people
- Enrich formal and informal collaboration at cultural level;
- A more active and transparent cooperation between public sector and SMEs;
- Foster collaboration for Cybersecurity and Certification and Standard;

Cyber Security Education and Training (Recommendation 7):

- Leverage existing learning facilities
- Provide funding for a yearly Academic "Capture the Flag" contest with participation from both EU and US.
- Provide funding for 10 year-long research visiting positions (post docs or similar) in the US that will enable young researchers from Europe to be educated on one security-related technology in the US.
- Provide funding for 10 year-long visiting positions in Europe that will allow US researchers to be hosted in the leading European Academic/Research centre and collaborate with the local researchers
- Provide funding for studies that will improve our understanding of the state of security research in Europe and US. For example, how prolific are EU researchers? How much do they publish in top conferences? How has this changed over the past years? What seems to be the main factors for such changes? Is there a gap between EU and US? How can this gap be filled?

Regulations (Recommendation 5)

- Work on regulations for Artificial Intelligence and Machine learning;
- Aim at resolving IPR implications.

Others

- More funding for outreach to reach civil society members;

5.11 Specific AEGIS recommendations for EU-US collaboration for the three focus domains

We have discussed several specific challenges for the three focus application domains and have provided our analysis with respect to the most crucial cybersecurity technologies. As for the topics of EU-US collaboration we propose to select those aspects of cybersecurity which require cross-organisational and international approach. The proposed topics will force the collaborating researchers to consider multi-stakeholder domains and face the issues caused by different regulations and administration.

5.11.1 Maritime

5.11.1.1 Proposed Topics for EU-US Collaboration for Maritime

- *Cybersecurity framework for complex maritime ICT environment*. The development of such a cyber risk management framework would ensure that every element in the complex maritime ICT environment (a vessel, a port, coast guard, etc.) is able to protect itself and provide its service in a secure manner.
- *Traffic control*. Cargo identification and tracking systems, heavily relying on IoT technology, are often a target of cyber-attacks. A good cybersecurity protection is required to ensure stable and reliable operation of the system at international level, where various entities, systems and regulations are involved.
- *International (and Inter-institutional) approaches to incident resolution and monitoring*. Efficient resolution of cyber incidents requires cooperation and trust of multiple entities.
- *Security system assessment, using risk-based approaches and right tools, such as attack trees and attack graphs*. Ships are increasingly using systems that rely on interoperability, digitization, integration and automation although shipboard computer networks usually lack boundary protection measures and segmentation of networks which are the most common targets for cyber-attacks.
- *Innovative cybersecurity training techniques*. Personnel in the maritime domain often have very little knowledge about cybersecurity and this weakness is exploited by attackers to penetrate into the system. Innovative training techniques are required to raise the awareness among the personnel, highlight the importance of cybersecurity and their role in the whole process, as well as teach them simple, usable and effective practices to reduce the chance to be manipulated by adversaries.
- *Deterrence and Collective Defence*. An overall defence posture is based on a broad range of options to respond to any possible threats to protect locations, vessels, personnel, and sea lines of communication. An overall strategy agreed with all the involved stakeholders must be set up in advance.

5.11.1.2 Challenges

- *Different regulations, such as the GDPR in Europe and the Cybersecurity Information Sharing Act in the US*, impose different (and, often, conflicting) requirements on the technology used by the maritime industry as many parts of the overall IT ecosystem are frequently moved from one jurisdiction to another one (e.g., ships and cargo).
- *Heterogeneous environment*. The overall maritime IT ecosystem includes many different parts, which belong to different owners (e.g., ports, coastal guard, ships, cargo, etc.) and have different internal IT systems, different goals, as well as cyber security techniques and practices applied.
- *National and international control*. Maritime research requires to consider the demands of national security and closely cooperation with governmental agencies (e.g., coastal control, navy forces, etc.).

- *Low level of cybersecurity knowledge*. The personnel have very low cybersecurity knowledge and often sees cybersecurity as something that distracts them from the core business. Such an attitude causes resistance to adaptation of additional cybersecurity measures as well as changing the attitude to cyber security practices.

5.11.1.3 Actions

Action	What to do	How to do it
A1	Establish a **Crisis Management Centre** to organize collective defence and deterrence activities among civil maritime stakeholders.	**Build an effective and efficient mission networking** across domain and nations, based on common management, processes, activities, technology, standards, education and training. Trust must be the keyword to initiate any collaboration. Periodical simulations must be scheduled to ascertain resilience and business continuity of the whole chain.
A2	**Establish Public-Private-Partnerships** for maritime cybersecurity.	Foster **cooperation among the maritime industry, research institutions and universities** to guide new technology development and to improve standardization and interoperability through an active provider involvement in PPPs programs.
A3	Develop a **cybersecurity "Attribution" program.**	**Increase coordination with the whole maritime ecosystem**, to actively collaborate with the legal enforcement agencies in order to enable identification, determent and stop cyber-criminal sources of attacks.
A4	**Improve cybersecurity' skills** and capabilities to protect maritime critical infrastructure.	**Organize joint training courses for managing risks** and link these training exercises with the US, forming a maritime cybersecurity triangle. Specific areas where this cooperation could be valuable include forensics training and judicial coordination in prosecuting cybercrimes. **Launch a multi-stakeholder-level training program** to educate the maritime operators how to behave and what actions to avoid during daily activities, to create, maintain and evolve capabilities in areas related to cybersecurity.

5.11.2 Healthcare

5.11.2.1 Proposed Topics for EU-US Collaboration for Healthcare

- *Health data exchange and privacy aspects* (including data usage control). Electronic Health Records (EHRs) are meant to be shared between different actors (patients, hospitals, pharmacies, etc.) with different roles and different levels of cybersecurity knowledge; it is essential to ensure that the data is used properly and only for the agreed and allowed purposes. All these considerations bring to the necessity of having a uniform cross-border platform that will enable a secure, private, and regulatory compliant data managing, storage and exchange.

- *Cybersecurity conformity assessment model*. Healthcare has a heterogeneous structure, including diverse entities (large hospitals, small clinics, laboratories, health insurance companies, etc.). These entities have different levels of protection (e.g., small clinics often lack skilled cybersecurity professionals to set up and manage their IT systems properly). Thus, for the overall cyber risk management, there is a need to establish a model for ensuring that the exchanged data is well protected once in the possession of a data processor.
- *Supply chain assurance model*. Cybersecurity of an IT system depends a lot on security of the software and hardware in use. There is a need for a model in which software and hardware providers assure its clients that their product is secure enough and that the vendor has a well-established and efficient patch and update process that will keep the product robust for long time of its usage.
- *Innovative cybersecurity training techniques*. The human factor is one of the weakest points in the eHealth domain. The personnel often consist of people who have very little knowledge about cybersecurity, who, nevertheless, play an important role in the socio-technical system of a Health organisation and often served as a point of entry (e.g., with social engineering attack) for attackers.
- *Securing legacy and new systems (security by design)*. New devices should be designed with the best security practices (e.g., following security and privacy by design approach). The existing healthcare devices should be appropriately secured (e.g., configured, patched, etc.) and/or protected by external security devices.
- *Safety/security issues* (like diagnostic invasive tools, robots). As more devices get access to the Internet, the possible impact of cyber events on safety of people becomes higher and higher. Furthermore, devices that have no access to the Internet, but relying on ICT elements (or some type of connection) should also be carefully analysed to fully understand possible impact of a cyber-attack on safety of a patient (or health provider personnel).

5.11.2.2 Challenges

- *Different regulations* (e.g., the Health Insurance Portability and Accountability Act - HIPAA, etc.) impose different (and, often, conflicting) requirements on the technology used by Healthcare organisations.
- *Heterogeneous environment with elements that have weak cyber security.* There is a need to ensure that various environments satisfy the minimal criteria for protection of data and ensuring correct level of data usage control. Currently, many IoT devices heavily used in healthcare have not been designed and implemented with security in mind and are not sufficiently protected against cyber-attacks.
- *Non homogeneous approaches to assessment, standardisation and certification.* There is no a suitable and widely accepted assessment and certification model that can certify if a system satisfies cybersecurity requirements.
- *Low level of cybersecurity knowledge and investment.* The personnel have very low cybersecurity knowledge and often sees cybersecurity as something that distracts them from the core business. Such an attitude causes resistance to adaptation of additional cybersecurity measures as well as changing the attitude towards cyber security practices. Also, the low levels knowledge of security and possible consequences lead to low investments to cyber security.
- *Obstacles for Data sharing*. Healthcare operates with sensitive data. This reason often prevents healthcare organisations to share the data about cybersecurity. With low exchange of cybersecurity information, healthcare organisations will not be able to learn the lessons from others and react quickly enough to the growing cyber-crime.

5.11.2.3 Actions

Action	What to do	How to do it
A1	**Devote more resources to healthcare R&I projects** that provide innovative methods for cybersecurity education and awareness raising.	Support **international cybersecurity training** and awareness event participation. Develop **good practices and tools for joint taskforces/workgroups** to define threats, priorities and establish a joint action plan for Healthcare cybersecurity.
A2	Provide a **framework for conformity security assessment** at international level.	Create a framework that ensures that **software and hardware coming from another county is secure** enough and does not contain "hidden" vulnerabilities. Next to the technical part, such a framework should also include a legal part that **enforces the liability** for dishonest vendors and producers along the entire supply chain.
A3	**Harmonize standards and legislations for cybersecurity of medical devices and software**.	Foster **government-industry collaboration** to harmonise legislations and standards related to cybersecurity. This will help manufacturers to develop secure devices which could be applied in various countries (i.e., for which a larger market will exist), as well as to allow buyers to have a larger selection of suitable producers/devices.

5.11.3 Financial

5.11.3.1 Proposed Topics for EU-US Collaboration for Financial Services

- *Fighting fake news.* News has great influence on the stock market. Consequently, so does fake news, which is deliberately spread by fraudsters in order to gain advantage from unexpected changes (and even panic) on the stock market. Preventing such news from appearing and spreading (especially, in social media) requires new models for social network influence, language processing, fake account detection, identifying and addressing deepfakes, etc.
- *Cybersecurity assurance, certification and responsibility.* Need to agree on common standards and certifications that facilitate data flow and trusted security among end-users along the whole supply chain. For example, the possibility to move a part of a business to the Cloud facilitates many business activities, which bring a number of cybersecurity questions: "how to select the most secure provider?", "how to be sure that the provider maintains its promises?" Furthermore, the crisis/incident management in such environment and sharing the responsibility for its mitigation is a problematic issue as well, in the international context, as many cloud providers are located in other countries comparing to their users.
- *Cyber Insurance*. Cyber insurance is a relatively novel way of distributing cyber security exposure, which gains popularity in the most cyber security advanced organisations. Moreover, by enforcing regulatory measures (e.g., targeting taxes, obligatory certification, increased liability, etc.) a government may influence the cyber insurance market to increase the welfare of the society in general (e.g., fast virus propagation prevention due to high security and fast reaction of key network elements). As Europe is lagging behind US in both

overall premium and number of insurance providers, collaboration in this field could help EU to raise its skills in the subject and foster a new promising market.

- *Data security and privacy*. Financial organisations collect huge amount of data by conducting their business (e.g., transactional data) as well as by collecting the information for their business (e.g., information about a potential insured). The privacy of users must be protected while the data are stored, processed and disposed.
- *Security of new distributed business models*. Distributed Ledger Technologies (DLT), such as Blockchain, need more dedicated risk evaluation, as for cryptocurrencies. For example, one issue to be dealt with is cryptography, which is essential for DLTs and could be challenged by the quantum technologies.

5.11.3.2 Challenges

- *Not homogeneous regulations*. Different regulations (e.g., Cloud act, GDPR, etc.) impose different (and, often, conflicting) requirements on the technology used by financial organisations.
- *Different governmental and institutional policies and goals.* Different policies in different countries restrain the law enforcement agencies differently, as well as various priorities of the agency may also affect its crime investigation process. Moreover, because of political reasons law enforcement collaboration could be blocked or slowed down.
- *Need to share data.* For a reliable security assessment approach and the whole cyber risk management process, large amount of sensitive data is required. This data, usually, is not available for researchers and kept secret as by those who owns the systems as well as by those who collects the data (e.g., insurers).
- *Not homogeneous approaches to security quality assessment, standards and certifications*. EU and US rely on different approaches to assess cybersecurity and manage cyber security risk. In US Cyber Security Framework (CSF) recently became one of the most popular approaches. EU does not have the unique standard, but the NIS directive and ISO 27001 are among the most known. Member States also have their own standards (e.g., BSI in Germany).

5.11.4 Actions

Action	What to do	How to do it
A1	**Agree and prioritize on finance certifications, standards and cyber security regulations** to be harmonized and how.	Create finance cybersecurity **collaboration frameworks** on able to operate under different jurisdictions without violation. Focus on projects that help to reduce the differences in legislations, standards and certification schemes, especially, regarding young technologies as **IoT, cloud and virtualization, DLT**, etc.
A2	Support R&I projects aiming for complex and distributing **crisis management actions**.	**Engage key actors** (e.g., law enforcement agencies, providers along the supply chain, ISPs, etc.), and consider the whole process including defining requirements and responsibilities, quick and coordinated reaction, and collaborative recovery. Commit funding agencies to support researchers and practitioners to meet and share best practices, requirements, challenges and innovative ideas.
A3	Foster **cyber insurance policies** in order to increase welfare of society as a whole and increase cybersecurity preparedness.	Focus on collaborative projects with the countries where the **cyber insurance market** is more developed and adopt them for the EU (e.g., US).

Action	What to do	How to do it
		Provide the way for researchers to **access available data** (e.g., to reports provided by organisations according to GDPR) about cyber-crime to estimate potential probabilities and impact for reliable risk management. Focus on the projects aiming for **premium discriminating** according to security levels.
A4	Encourage **information sharing** between governmental agencies at national and international levels.	Promote **engagement in the information sharing** initiatives (e.g., like FI-ISAC), providing researchers access to this data. Support the projects that aim to encourage organisations to share their data (rather than just consume).

5.12 Privacy

Privacy and security usually treated together as they are very similar in many aspects and achieving privacy often means installation of security countermeasures. JRC taxonomy is not an exclusion in this case (as well as other, e.g., RSA of NIS WG3) and does not allow singling out privacy only issues, most of which are treated under the umbrella of Data Security and Privacy technology (rated as one of three most important technologies for research in our analysis). In this section, we try to provide separate insights into privacy by analysing the following documents:

- NIST Privacy Framework: An Enterprise Risk Management tool (draft)[43];
- Security Research Agenda of NIS[44].

5.12.1 Proposed Topics for Privacy R&I

- *Privacy Risks Management Framework.* So far the main attention of system managers were mostly focused on security while performed cyber risk management activities. Naturally, well known standards, like ISO 27001/2 and NIST CSF devote considerable attention to privacy as well, but we still lack of a comprehensive and consistent privacy risk management framework. Such framework is under the development in USA (i.e., NIST Privacy Framework) while Europe, although recognizes the need for one, still does not have it.
- *Privacy Enhanced Technologies (PET).* Although there are many implementations of privacy enhanced technologies, many of them lack usability and user friendliness. Moreover, we should aim for the technologies which allow user to control its privacy. PET should be cost effective and widely applicable, helping users to maintain their privacy even if forced to use specific service/software/hardware (e.g., because of no suitable alternative).
- *Privacy by design.* In order to ensure privacy, we need to integrate it into the overall process of software development, making sure that the privacy is considered at every stage. Especial attention should be devoted to composition of PET technologies to ensure that such composition is simple, efficient and still ensures privacy properties. This require formalization of privacy requirements, their verification and collection of suitable evidence which can be used to convince external parties in fulfilment of privacy requirements.

[43] https://www.nist.gov/sites/default/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf

[44] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-draft-v02.63/at_download/file

- *Partial identities.* Today IT services are used by people for multiple purposes (healthcare, sport, entertainment, work, citizen duties, etc.). It is the right of people to avoid sharing some of their activities (e.g., entertainment) to others parties involved in another aspect of their life (e.g., work). Thus, people should be able to use different identities to ensure that their private information is shared only among target group of individuals. This topic also should include the authentication procedures that avoid using identities (e.g., using attributes). Next to minimizing potential linking of identities, these mechanisms also may help to minimize the amount of (private) information shared with and collected by external parties.

5.12.2 Actions

- *Invest in development of Privacy Risk Management Framework for Europe.* This work should also be based on the recent advances in European legislations (e.g., GDPR, Privacy Act, etc.). Collaborate with US colleagues to develop a compatible framework with the one being developed in US.
- *Support analysis of requirements of end users for PET.* Users should be able to apply the developing technologies for privacy. They should have enough knowledge and capabilities, moreover, they should be able to continue using the services/software/hardware which are essential for their lives. Cultural differences should be taken into account.
- *Study incentives for usage of PET and ways to foster these incentives.* Software/hardware producers and service providers are not primarily interested to embed PETs or enforce privacy-by-design principles. There is a need to study the incentives which could influence adoption of privacy-enforcing practices.
- *Raise privacy awareness among citizens.* There is a large asymmetry in understanding the value of information between data owners and data collectors. People often do not understand the ways their private information can be abused, nor do they often know how to protect themselves. Innovative ways to explain the need for maintaining privacy and ways to achieve it in the modern world are required. This approach should also help people to understand the importance and help enforcing various privacy legislations.

6 CONCLUSIONS

This deliverable provides the results of the AEGIS desktop analysis of various cybersecurity and privacy programmes across the Atlantic. We have found that cybersecurity topics such as *Security Management and Governance; Data Security and Privacy; Education and Training; Assurance, Audit and Certification;* and *Network and Distributed Systems* get the most attention from funding programme managers as well as from the research community´s point of view. *IoT* has been found to be the most demanded ICT technology from a cybersecurity and privacy point of view, followed by *Cloud, Mobile, Big Data*, and *Operating Systems*. The concrete Applications are dominated by *Energy, Public Safety, Transportation, Financial Services* and *Healthcare.* In general, these results coincide pretty well with the results of the AEGIS survey on cybersecurity and privacy R&I priorities.

We have applied the results of the analysis to the three AEGIS focus application domains – Healthcare, Financial and Maritime – to find out how well the most important CSP issues in all three domains are addressed by current priorities. Our analysis shows that most of the topics classified as highly important priorities are well covered by the available programmes. Nonetheless, *Cryptography* has received less attention than required, which should be addressed in future programmes as cryptography often lies in the basis of many security features. With the rapid development of ICT technologies (e.g., IoT or quantum computing), requirements for these security features change and may violate prerequisites for existing cryptographic primitives. In addition, the analysis has found that the EU puts more emphasis on *Assurance, Audit and Certification* and *Trust Management, Assurance, and Accountability*, while the US devotes little attention to these topics. For *Identity and Access Management* and *Software and Hardware Security Engineering*, the situation is opposite.

The deliverable presents a number of practical recommendations outlining the topics for possible EU-US collaborations in cybersecurity and privacy R&I. It also highlights the need to improve collaboration procedures between both regions in general, particularly when it comes to research funding programmes.

7 ANNEX 1 AEGIS TAXONOMY

In scope of AEGIS project, a taxonomy for cybersecurity and privacy has been developed in the beginning of the project. The taxonomy was further substituted by the one developed by JRC in order to avoid further mismatching of our results with the further activities of the EU Commission (that was going to use JRC taxonomy).

In this Annex, we provide the first version of AEGIS taxonomy.

7.1 Our Taxonomy

There are several approaches to definition of taxonomies of cybersecurity taxonomy. After analysis of several of them, we have found that the state of the art often mix pure cybersecurity technologies, application of these technologies in various application domains, and cybersecurity approaches for securing ICT technologies. In fact, the latter two cases are just application of cybersecurity technologies to specific ICT technology or Application domain. One approach to definition of taxonomy could be to focus on pure cybersecurity technologies only. On the other hand, ICT technologies and Application domains often characterized by their own peculiarities and limitation, which make application of cybersecurity technologies to them unique tasks. We have decided to keep all these three domains in our taxonomy, but separate them.

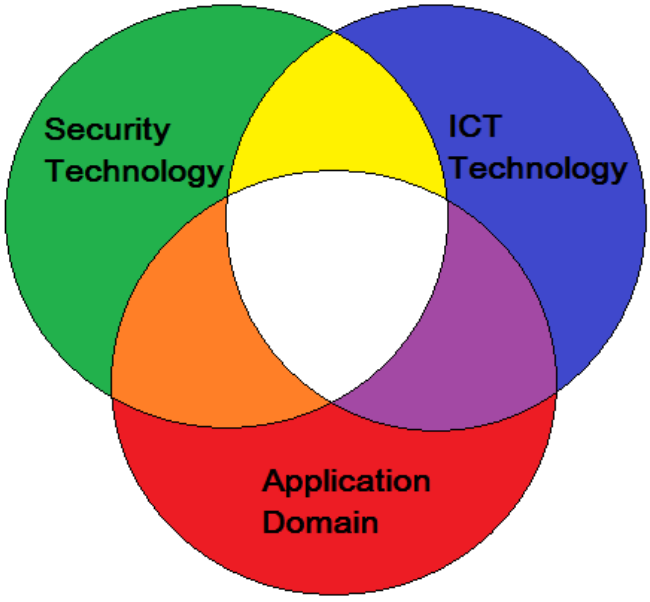


Figure 3: Cyber security R&I areas within our taxonomy

Cybersecurity Technological Domain

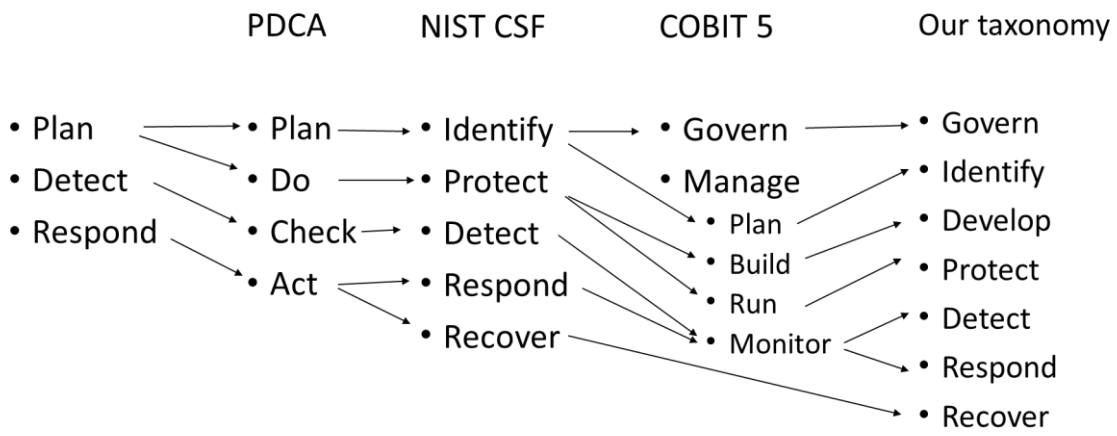
Our Cyber Security Technological domain is split in accordance to phases of cybersecurity/risk management life-cycle. Such an approach ensures the comprehensive coverage of the taxonomy.

Our taxonomy includes 7 general steps:

- Govern
- Identify
- Develop
- Protect
- Detect
- Respond

- Recover

Such high level categorisation follows the main standards in cybersecurity and can be derived also from the well-known Plan-Do-Check-Act cycle applied to cybersecurity area.



For every high-level cybersecurity technological category we define a set of specific topics.

A. Govern

Activities which organize the work, assigns responsibilities and specify the goals for the security system.

- **A.1 Organization of information security –** specification of roles and responsibilities for information security for all employees of the organization and its partners (including all security processes: access control management; physical access control process; credentials/access rights management; event detection process; vulnerability management process; event response process; recovery process; etc.); notification about the assigned responsibilities; coordination of the security activities; communication of security posture to the highest managers; security budget management;
- **A.2 Compliance and legal issues –** identification and understanding of the relevant security standards and legal obligations (e.g., data protection regulations); embedding the required legal and compliance requirements into security management routine; ensuring that
- **A.3 Security Policies –** definition of security policies and verification of their importance for achieving security goals; specification of security policies (e.g., in manuals and codes of conduct); ensuring that employees are familiar with the relevant policies and follow them; periodic revision and improvement of security policies; definition of the physical access procedures; secure configuration definition; control mechanisms and procedures implementation; back-up procedures defined, enforced and timely executed, specification of a response and recovery plans; vulnerability management procedures defined.

B. Identify

Activities which help to identify the valuable assets, analyse security threats and understand the security needs.

- **B.1 Asset management** – activities related to identification and prioritization of various security assets, like hardware, software platforms and applications, communication and data flow, external information systems;.

- **B.2 Business environment -** understanding the role of the organization in the supply chain, its criticality for and dependency on others; prioritization of organization objectives.
- **B.3 Risk Assessment -** understanding the possible malicious actors and events which may negatively affect the security and privacy of the organization; study of their capabilities, resources, and knowledge; identification of the vulnerabilities which may help malicious actors and events to occur; estimate possible impact and probabilities of cybersecurity incident occurrence; determine risks, prioritise them and define suitable treatment.
- **B.4 Risk Management Strategy –** the risk management processes are defined, enforced and managed; the residual risk is understood, accepted, documented and communicated to the overall risk/company managers. This activity also includes risk management for suppliers, i.e., understanding the information systems, components and services of the supplier, the possible risks, and development contracts and agreements with partners. The contracts and agreement muct address the identified risks, specifying the required measures, assessment and testing procedures as well as response and recovery plans.

C. Develop

Activities which relate with the secure development of a system, starting from the early stage of requirement elicitation and ensuring that these requirements are fulfilled by the implementation.

- **C.1 Define requirements** – define security requirements out of company/target objectives, business goals, legal and compliance requirements, prioritized risk, etc.
- **C.2 Secure development and support –** secure design and architecture design (security-by-design and privacy-by-design); definition and enforcement of secure system-development life-cycle;
- **C.3 Maintenance and assurance –** methods (also, formal) for assurance that security goals and requirements are properly fulfilled by implementation; proper maintenance of assets and logging.
- **C.4 Testing –** active testing to determine the weak defense and vulnerabilities; software security testing; system penetration testing; etc.

D. Protect

Various miscellaneous activities which prevent cybersecurity and privacy threats from occurring.

- **D.1 Access control –** trust management; key/credentials management; identities/roles/permission identification, analysis, assignment, and management; physical access control; remote access control;
- **D.2 Awareness and training –** raising cybersecurity and privacy awareness among high level managers as well as among employees; security training of personnel;
- **D.3 Data security –** protection of stored and transmitted data (including encryption); proper management procedures for asset management (insertion/removal, modification, transfer, etc.) are established; maintaining the proper availability level; integrity checking mechanisms.
- **D.4 Privacy-Enhancing Technology -** privacy-enhancing technologies; data leakage protection; mechanism for privacy-preserving computation, access and exchange; minimal access rights;
- ensuring the right purpose of data usage; data/media distraction/deletion;
- **D.5 Protective Technology –** events are logged and audited; enforcement of access control; protection of communication and networks;

E. Detect

These activities help to detect ongoing or occurred threats.

- **E.1 Anomalies and Events –** definition of the normal behavior; analysis of abnormal events; event aggregation and correlation; possible incident impact analysis;
- **E.2 Security Continuous Monitoring –** detection of abnormal events; physical events monitoring; personnel activities monitoring; vulnerability scans; malicious code detection; unauthorized access detection; monitoring partner activities;
- **E.3 Detection Processes –** definition of detection processes and their compliance with security policies and responsibilities; communication of detected events;

F. Respond

These are the activities that help the organization to react efficiently on the occurred threats in order to reduce the impact.

- **F.1 Response Planning** – ensure that the response is executed according to the response plan.
  F.2 Communications and incident sharing – report the event according to the plan; share the information about the incident through the incident sharing programme the organization is involved in.
- **F.3 Analysis** – investigate events; evaluate the impact; perform forensics; categorise incidents
- **F.4 Mitigation** – restrain the indecent; mitigate the incident; update the risk assessment results taking the new knowledge into account
- **F.5 Improvements** – update the response plan with new lessons learned;

G. Recover

This set of activities specifies an efficient way to recover the system from an attack back to the normal functional state.

- **G.1 Recovery Planning** – ensure that the recovery is executed according to the recovery plan
- **G.2 Improvements** – update the response plan with new lessons learned;
- **G.3 Communications –** manage public relations; repair reputation; report to higher managers

ICT Technological domain

We have selected several topics from the general ICT technologies which require specific cybersecurity attention.

- Web Services and Cloud
- Big Data
- IoT
- Operating Systems
- High-Confidence Software and systems
- Networks
- Mobile Devices
- Cyber-physical systems
- Industrial control systems

Application domain

The following application have been found the most challenging from the cybersecurity point of view. We do not want to say that other application categories do not deserve attention of cybersecurity, but would merely like to underline the importance of the listed categories:

- E-Government
- Industry 4.0
- Smart transport/automotive
- Banking and finance
- eHealth
- Energy (smartGrid)
- Smart Environments
- Telecommunications/ICT services
- Water treatment systems
- Agriculture
- E-education
- Robotics
- Nuclear

7.2 Mapping of our Taxonomy with Others

NIST CSF

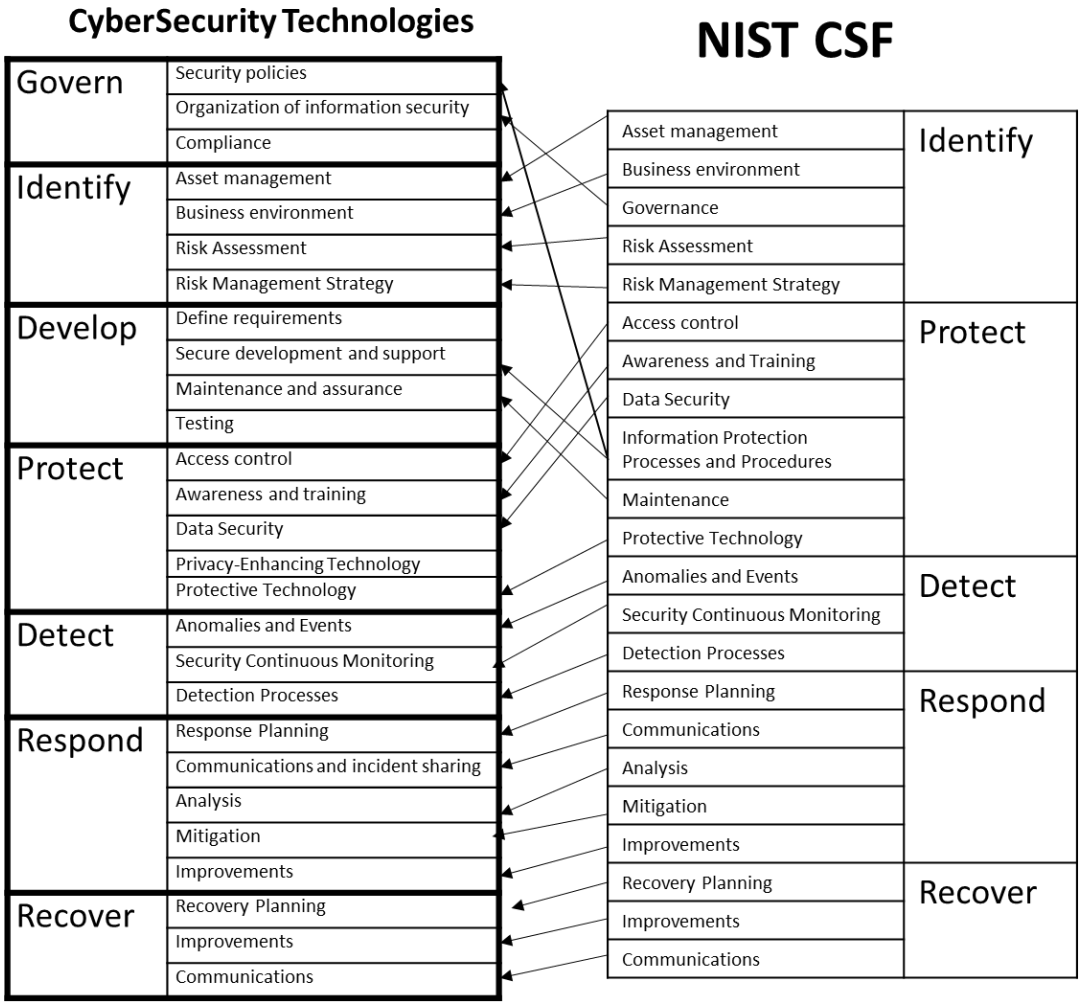


Figure 4: Mapping of our cybersecurity technologies to NIST CSF.

The mapping of our cybersecurity technological domain to NIST CSF framework is pretty straightforward as we were inspired by the last developments of NIST. The main difference is in two new high level categories which were singled out: Govern and Develop. Nevertheless, these new categories require only some regrouping of specific technologies. We also may see that a couple of technologies are not explicitly covered by NIST framework (e.g., Compliance, Definition of Requirements, and Privacy-Enhancing Technologies).

ISO 27002

Figure 5: Mapping of our cybersecurity technologies to ISO 27002

If we compare our methodology with the most known standard in cybersecurity ISO 27001/2, then we will see that our taxonomy covers well the categories of this ISO standard. One may notice the poor coverage of Risk Assessment and Risk Management Strategy. This could be explained by the fact that the ISO standard underlines the necessity of risk management and analysis separately, and highlights that the standard itself should be applied addressing identified risks. In other words, risks assessment in ISO 27001 is the driven force, rather than a mean. Also, there is no specific component in the ISO standard that covers Data Security explicitly. Finally, some ISO categories could be mapped to the high level categories in our taxonomy (see Develop, Detect, Respond and Recover), rather than a specific technology. The mapping between technologies can be achieved if we go deeper into ISO categories, but this is not the main goal of our current study.

COBIT 5

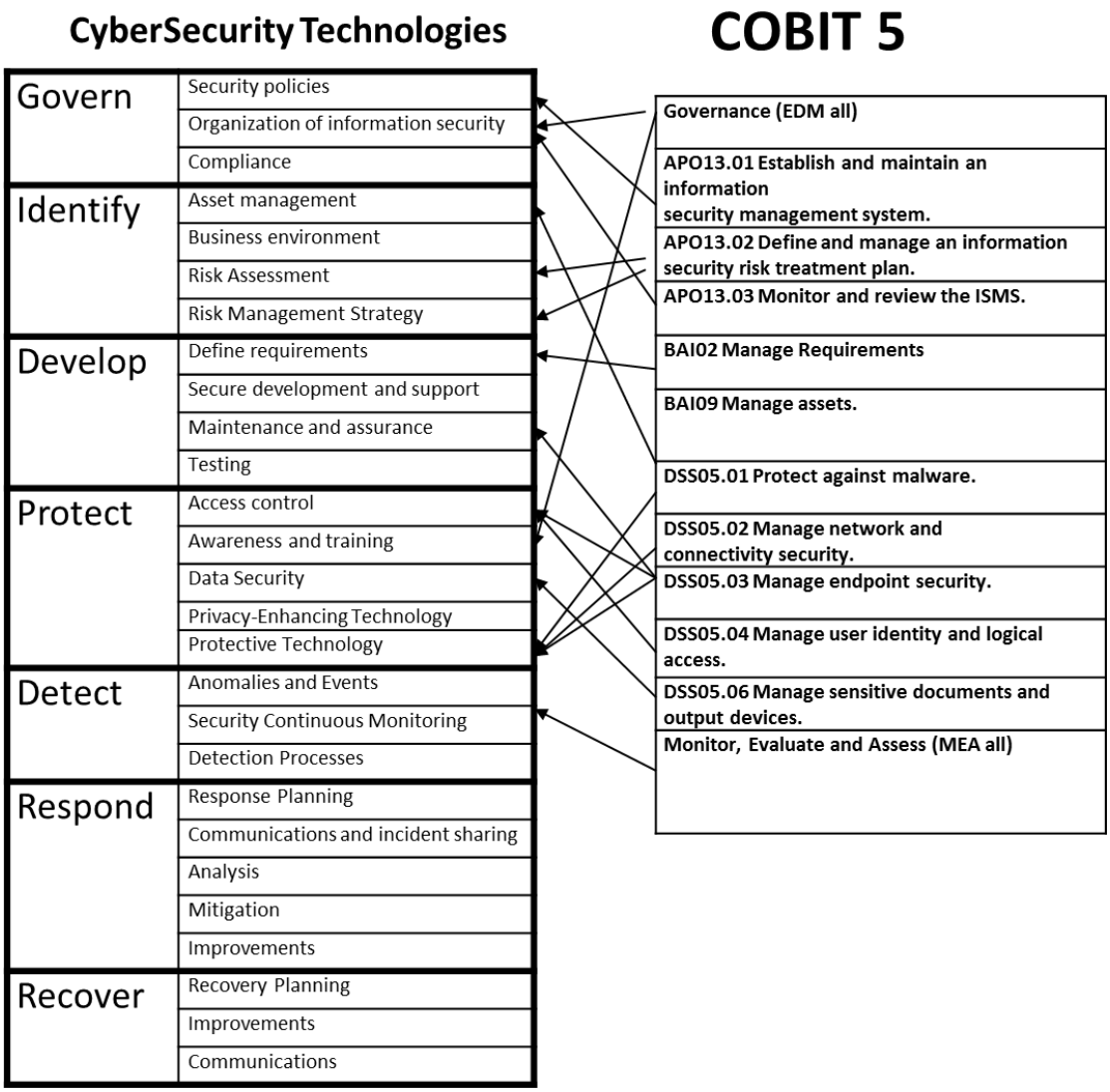


Figure 6: Mapping of our cybersecurity technologies with COBIT 5.

COBIT 5 is a general management standard for IT systems and it includes several practices which are dedicated to security (all DSS05 practices) and others that cover cybersecurity as one important aspect (e.g., monitoring). COBIT 5 covers well the first five categories, but misses Respond and Recover. Also COBIT 5 does not focus on development of secure applications, but mostly targeting application usage and maintenance. Detection is also addressed by the standard only as a general practices (MEA), without paying much detailed attention to security aspects.

NIS WG3 Landscape

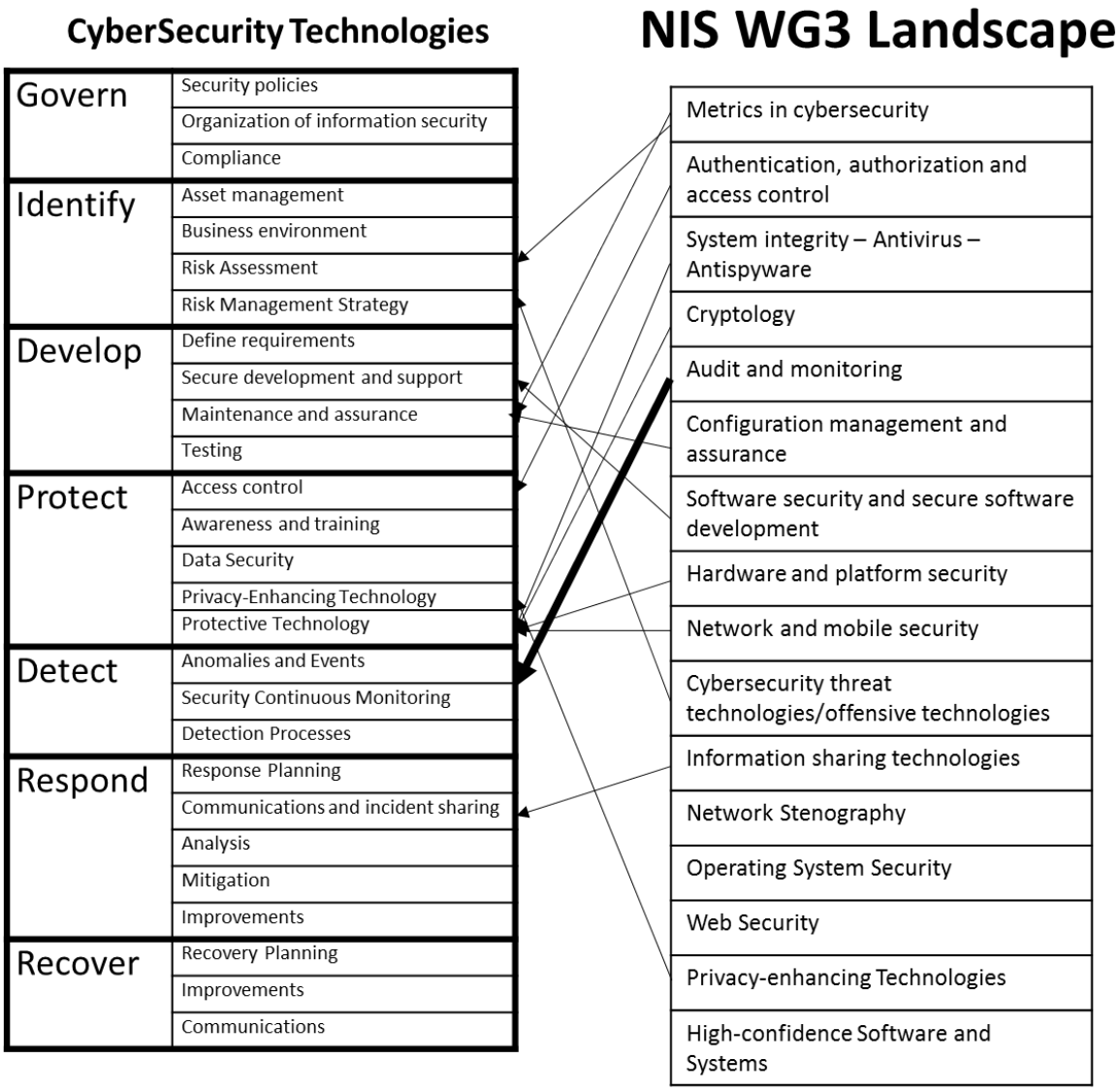


Figure 7: Mapping of our cybersecurity technologies to NIS WG3 Landscape

NIS WG3 Landscape, as it follows for the mapping in Figure 7, mostly focusses on secure development, protection and detection ("audit and monitoring" is a generic category which covers most of Detect category in our taxonomy.). Response is covered only by information sharing technologies and Identification is limited to risk metrics and analysis of offensive technologies. Such categories as Governance and Recovery are not covered at all.

The RSA produced by NIS WG3 is also mostly focusses on just a few core cybersecurity categories (Develop, Protect and Detect). See Figure 8.

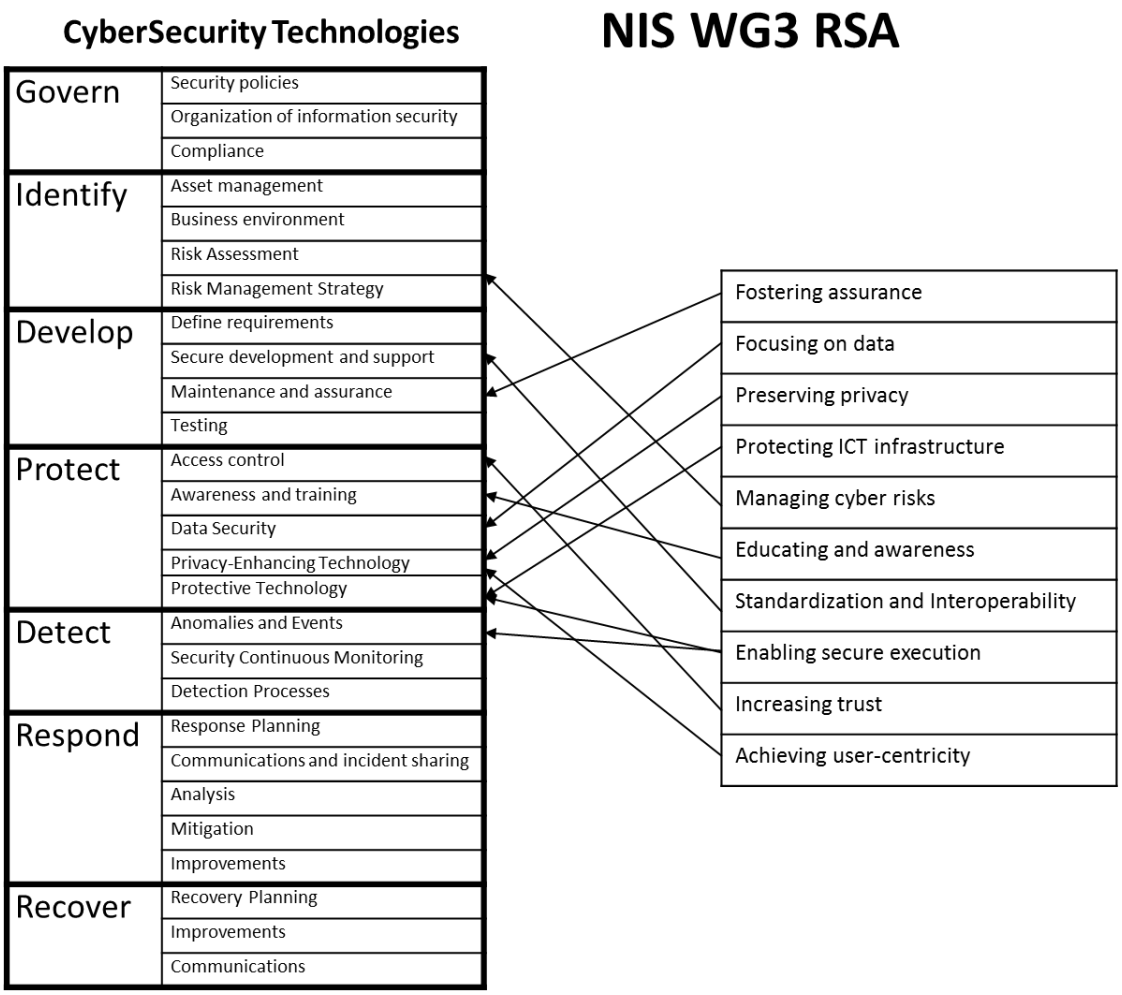


Figure 8: Mapping of our cybersecurity technologies with NIS WG3 RSA

cPPP

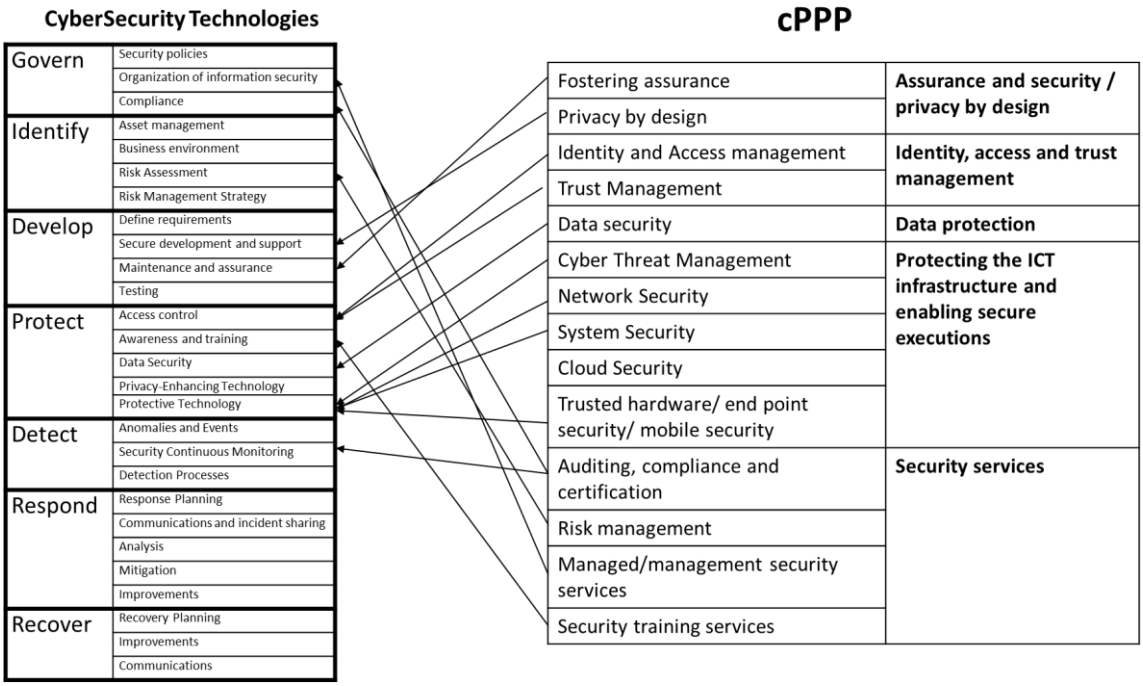


Figure 9: Mapping of our cybersecurity technologies with cPPP

The taxonomy of topics for research proposed by cPPP, as well as NIS, focuses on Protection, Development (foster assurance and a wide topic covering may aspects of secure development) and Detection (although, the last one also focuses on compliance checking). Also, cPPP underlines the importance of risk management in Identifying cybersecurity problems, as well as governance of security.

7.3 Comparison of the JRC Taxonomy with Others

Our Taxonomy

Now we are going to compare our Cyber Security Technology Domain with the one from JRC.

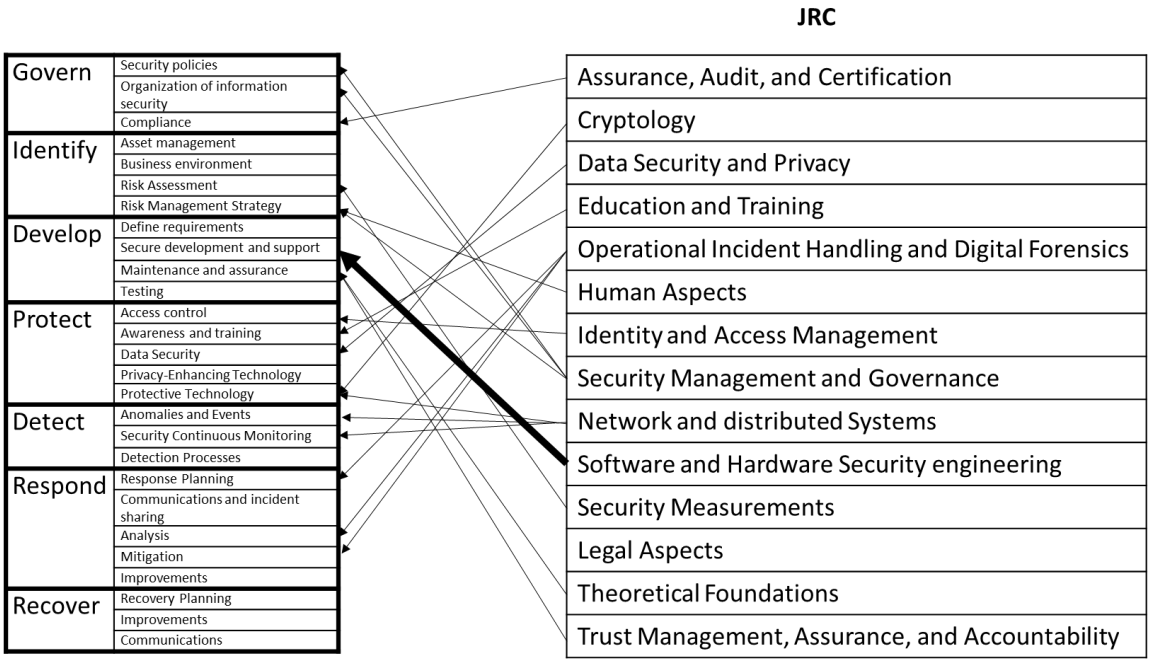


Figure 10: Mapping of our cybersecurity technologies with cybersecurity technologies of the JRC Taxonomy.

If we try to compare our cybersecurity technologies with the ones defined by JRC we will that JRC covers well first five categories (although JRC focusses more on risk management, leaving preparation steps, like asset management and business environment assessment out). Response is also well covered, but JRC does not include sharing information about the incident. Finally, JRC does not focus on recovery part.

On the other hand, JRC also includes Legal Aspects of security, which we found out redundant for our taxonomy, which focuses mostly on technical, rather than legal aspects of cybersecurity. Also, JRC devotes more attention to human aspects, considering both attacker modelling and user modelling (including social-technical models). Partially, our methodology considers attacker modelling in scope of risk assessment.

cPPP

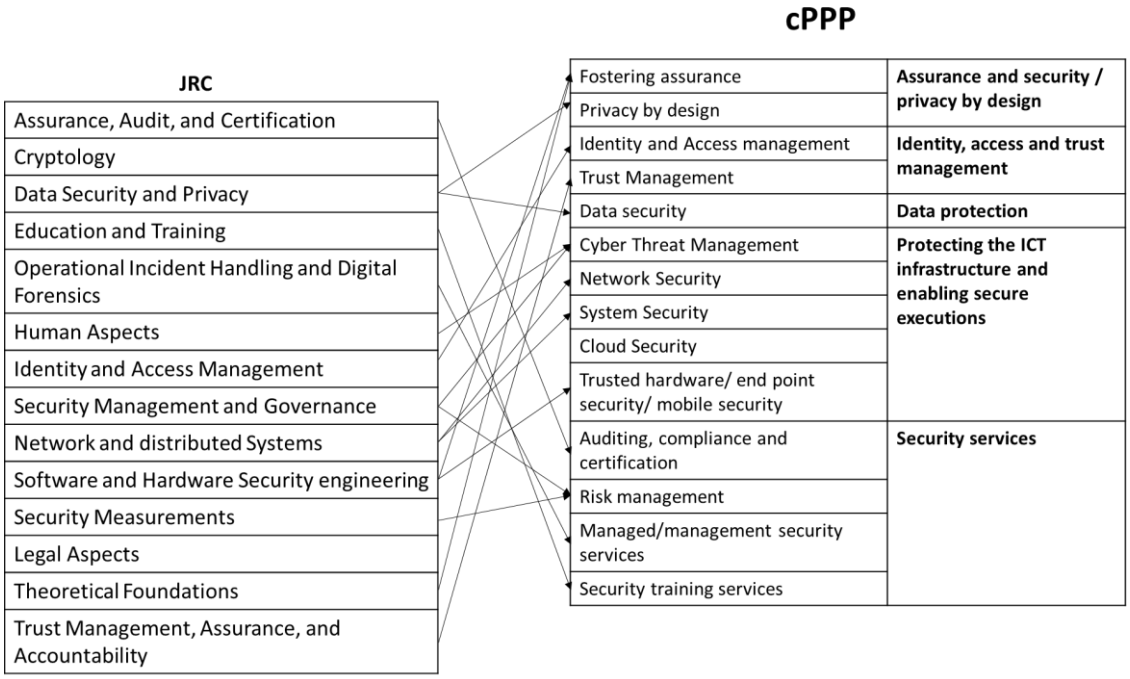


Figure 11: Mapping of cybersecurity technologies of JRC with cPPP

IF we compare JRC with the cPPP topics, we will find that these two taxonomies map very well, with only some misalignment. For example, cPPP does not focus on cryptography; although it underlines its importance, no specific topics for cryptography are considered. Also JRC has the focus on attacker modelling and user analysis, which only partially covered by Cyber Threat Management of cPPP. Finally, JRC also considers legal aspects of security.

NIST CSF

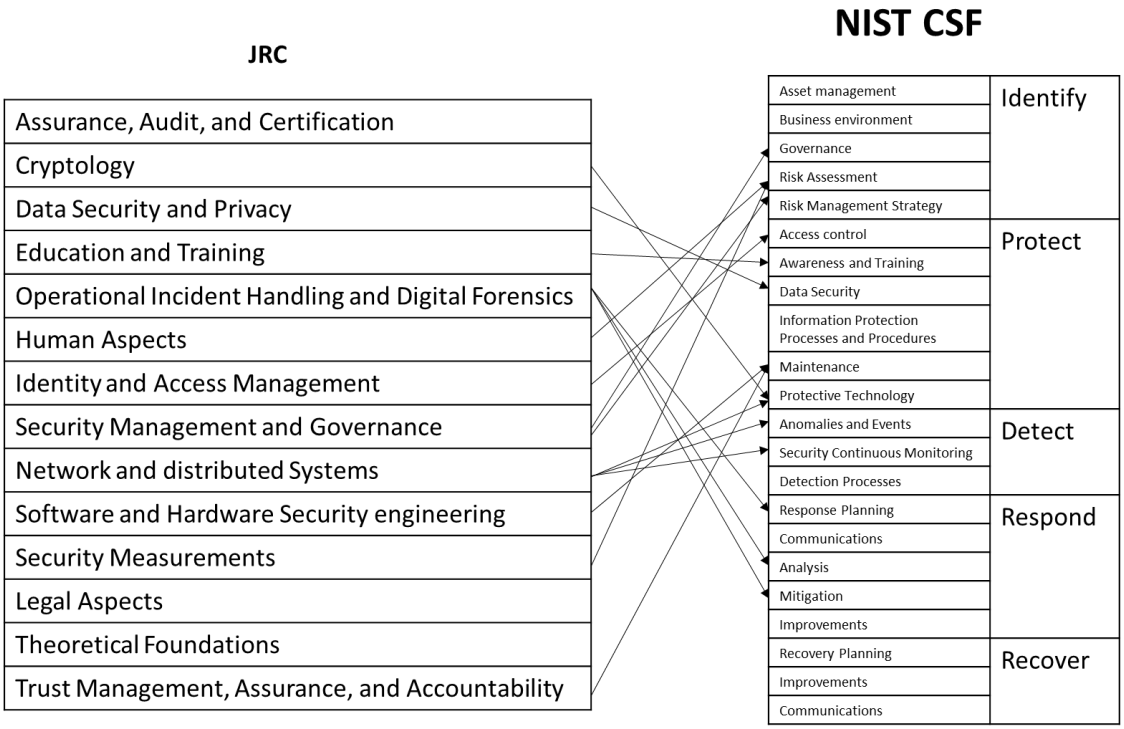


Figure 12: Mapping JRC and NIST CSF.

JRC and NIST CSF look slightly different. JRC does not cover recovery part and miss some practical steps (e.g., business environment analysis, communication of detected incidents, improvement after an attack). On the other hand, JRC has focus on certification, which is not in CSF. Also, theoretical foundations and legal aspects are no captured by CSF.

8 ANNEX 2 AEGIS INTERVIEW FORM

AEGIS Interviews with Key Stakeholders - Guidelines

Objective: To gather insights on the EU/US landscape on cybersecurity and privacy and on the AEGIS recommendations for transatlantic R&I cooperation.

1. **AEGIS has identified the following action areas for EU-US collaboration. Do you think these areas are the most relevant? If so, why? If you disagree, please explain why you feel this way.**

a. Top 5 Cybersecurity Areas

- *Security Management and Governance*
- *Data Security and Privacy*
- *Education and Training*
- *Assurance, Audit and Certification*
- *Network and Distributed Systems*

---

b. Top 5 ICT Technologies

- *Internet of Things*
- *Cloud and Virtualization*
- *Mobile Devices*
- *Big Data*
- *Operating Systems*

---

c. Top 5 Applications

- *Energy*
- *Public Safety*
- *Transportation*
- *Financial Services*
- *Health*

---

2. **AEGIS makes the following recommendations for EU-US collaboration in cybersecurity and privacy R&I. Do you agree with these recommendations? If so, why? If you disagree, please explain why you feel this way.**
    - *Take an international approach to cybersecurity;*
    - *Invest in international cybersecurity projects;*
    - *Establish coordination between funding programmes;*
    - *Reduce legislation barriers for collaboration on cybersecurity and privacy;*
    - *Promote information sharing for cybersecurity;*
    - *Foster collaboration in cybersecurity education and training; and*
    - *Support securing Critical Infrastructure.*

3. **Would you suggest any other recommendation to improve EU-US collaboration in cybersecurity?**

9 ANNEX 3 GLOSSARY

Application domain (aka sector, application, domain) – a category of industry. Various industries have special requirements for cyber security and rely on different ICT technologies. In our work, we underline the importance of application of cybersecurity to specific application domains, considering application domains as one of vectors of our analysis.

Attack- attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset [ISO 27000:2016]

Desktop analysis – an analysis which is based on evaluation of existing documents. The documents in our desktop analysis are various cybersecurity research programmes specifications, cybersecurity research agendas, governmental directions for research.

Cybersecurity research agenda – a set of guidelines and priorities for cybersecurity research developed by a certain entity.

Cybersecurity technology topics (aka cybersecurity research domain) – a high level cybersecurity category related to a specific cybersecurity aspect. It is one of three vectors in our analysis.

Control - measure that is modifying *risk* [ISO 27000:2016]

ICT Technology (aka Applications and Technologies) – a category of ICT that relates to specific functionality. It may include hardware (e.g., mobile), software (e.g., operating systems), service (e.g., cloud) or computational (e.g., big data and AI) elements, all or some. In our work, we underline specific cybersecurity challenges to be addressed by application (and/or adaptation) of specific cybersecurity technologies. It is one of three vectors in our analysis.

Information security - preservation of *confidentiality*, *integrity* and *availability* of information [ISO 27000:2016]

Policy - intentions and direction of an *organization* as formally expressed by its *top management* [ISO 27000:2016]

Risk - effect of uncertainty on objectives [ISO 27000:2016]

Risk assessment - overall process of risk identification, risk analysis and risk evaluation [ISO 27000:2016]

Risk management - coordinated activities to direct and control an *organization* with regard to *risk* [ISO 27000:2016]

Threat - potential cause of an unwanted incident, which may result in harm to a system or *organization* [ISO 27000:2016]

Vulnerability - weakness of an asset or *control* that can be exploited by one or more *threats* [ISO 27000:2016]

aegis accelerating EU–US Dialogue in Cybersecurity and Privacy

Quotation:

When quoting information from this report, please use the following phrase:
"Benchmarking report on Cybersecurity and Privacy landscape in EU and US. AEGIS project."

Consortium:

inmark europa
Consiglio Nazionale delle Ricerche
Waterford Institute of Technology
Hewlett Packard Enterprise
european american chamber of commerce new jersey
THE PROVIDENCE GROUP
RUTGERS

aegis-project.org linkedin.com/company/aegis-project @aegis_cyber