White Paper on Research and Innovation in Cybersecurity

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CSA	Coordination and Support Action
CSP	Cybersecurity and Privacy
JRC	Joint Research Centre
NITRD	Networking and Information Technology Research and Development Program
SaTC	Secure and Trustworthy Cyberspace
NSF	National Science Foundation
DHS	Department of Homeland
NSTC	National Science and Technology Council
NIS	Network and Information Security
cPPP	Contractual Public Private Partnership
ECSO	European Cyber Security Organisation
R&I	Research and Innovation
SRA	Strategic Research Agenda
SRIA	Strategic Research and Innovation Agenda
ENISA	The European Union Agency for Network and Information Security

EXECUTIVE SUMMARY

The effect of the development of information technology (IT) and its rapid penetration and reshaping of the modern industry and society is, to a large extent, similar on the both sides of the Atlantic. Both the European Union (EU) and the United States (US) face similar cybersecurity and privacy challenges, which require additional research and innovation (R&I) ideas. Thus, it is not very surprising that different cybersecurity and privacy (CSP) funding programmes have similar focus areas. At the same time, for the funding programme managers, it is important to understand where the research interests of the EU and US coincide, i.e., acknowledged by both jurisdictions as a promising topic.

It is also crucial to understand where the focus areas diverge, which could mean either an excessive funding of the area by one side or underfunding of an important area by another (or some combination of both). Naturally, different legal, political, cultural and business landscapes play a role in shaping the priority areas for research and innovation. This was also to be taken into account while undertaking a comprehensive comparison of different R&I programmes.

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 White Paper in an attempt to capture the current landscape of R&I in cybersecurity and privacy on both sides of the Atlantic.

This White Paper 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[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*

[1] The results of the survey could be found in "AEGIS Report on Cybersecurity and Privacy R&I Priorities for EU-US Cooperation" and can be downloaded from the AEGIS web-site through the following link: http://aegis-project.org/cybersecurity-downloads/

Access Management and *Software and Hardware Security Engineering*, the situation is opposite.

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

The target audience of this White Paper 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.

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

In this section, we analyse EU and US priorities in cybersecurity and privacy as well as the coverage of various cybersecurity and privacy topics in their R&I programmes. We map the priorities with the Joint Research Centre (JRC) taxonomy [2] for cybersecurity and analyse the attention devoted by EU and US to cybersecurity and privacy.

The JRC's taxonomy defines three vectors for categorising CSP R&I directions. It is important to note that we use slightly different names for the three vectors.

- Cybersecurity Research Domains;
- Application and Technologies; and
- 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.

1.1 Selected documents for the desktop analysis

1.1.1 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[3] on the 1st December, 2016;
- Federal Cybersecurity Research and Development Strategic Plan[4] (released in December 2016);
- Secure and Trustworthy Cyberspace programme[5] (SaTC) of National Science Foundation (NSF);

[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 . We have found that the changes with respect to version 3.0 are related mostly to renaming and enlarging the lists of Applications and Sectors. They do not have a large impact on the results of our analysis.

[3] 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.

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

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

- Cyber Security Division[6] (CSD) programme of Department Homeland Security (DHS);
- DARPA programmes[7];
- IARPA programmes[8].

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[9] 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.

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[10] contains information about the investments of different agencies in cybersecurity and information assurance.

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

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**

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

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

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

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

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

(DHS) make significant investments in cybersecurity and privacy R&I and have detailed research programmes available. Therefore, they are also considered in our analysis.

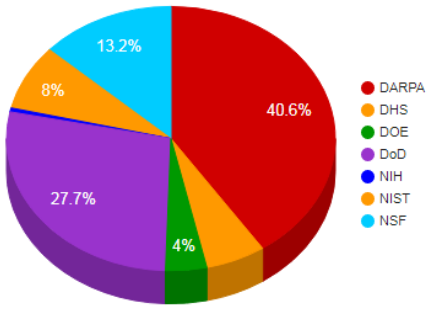

Figure 1: US Agencies cybersecurity budget distribution in 2018

1.1.2 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.

- Horizon 2020 R&I Funding Program[11];
- The Network and Information Security Platform initiative[12];
- Contractual PPP on cybersecurity[13] (cPPP) and its supporting organisation European Cyber Security Organisation[14] (ECSO) initiative;
- The activities of the European Union Agency for Network and Information Security[15] (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[16]**, eIDAS, GDPR and Directive 95/46/EC.

---

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

[12] 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

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

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

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

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

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[17] 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.

1.2 Unified analysis with the JRC taxonomy

In order to determine the overall priorities in the EU and the US, we have combined the results of our desktop analysis and our survey. During the desktop analysis, the priorities highlighted in every document mentioned in Section 1.1 were mapped on to the corresponding JRC category. Then, we assigned a weight for every document to reflect its impact on R&I in both countries and computed a weighted sum per JRC's category. In short, every value our analysis produced (the values belong to the interval [0;1]) reflects the priority of the category for the EU and the US.

The second source for the priorities is the online survey which was carried out by AEGIS from 10 May 2018 to 31 May 2018. The questionnaire was answered by a total of 130 relevant stakeholders in the cybersecurity and privacy R&I and policy fields. Most respondents were individuals who worked at universities and research centres (44,3%) and private companies (31,0%). Nonetheless, there were also participants from Small and Medium-sized Enterprises (7,0%), government organizations (6,2%), NGOs (3,9%) and associations (3,1%). The respondents were asked to provide CSP priorities for Cybersecurity Technology topics, ICT Technologies and Applications[18] by classifying it with a value between 1 and 4, where 4 indicated the highest importance. A more detailed breakdown of the survey results can be found in the report on the AEGIS website[19].

In order to determine overall priorities (i.e., the total score) of the EU and the US, we aggregated the results from our desktop analysis and the results of our survey by taking the average value (the results of the survey were first normalised to get the values in the interval [0;1]). In cases where our survey did not address a topic, we left the corresponding cell blank and propagate only the value of the desktop analysis. All final tables are sorted by the total average value (for the EU and the US).

1.2.1 Cybersecurity Technology Topics

As shown in Table 2, 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.

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

[18] As the survey uses a mixed terminology of JRC and NIST, some terms used in the survey are different with respect to the one used in this White Paper.

[19] See "AEGIS Report on Cybersecurity and Privacy R&I Priorities for EU-US Cooperation" at the AEGIS website through the following link: http://aegis-project.org/cybersecurity-downloads/

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 2: Total ranking for cybersecurity technology topics

CSP 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	0.795	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	0.842	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	0.782	0.56	0.79	0.75	0.77
Trust Management, Assurance, and	0.47	0.86	0.66	0.73	0.935	0.83	0.21	0.82	0.52
Human Aspects	0.51	0.79	0.65	0.38	0.797	0.59	0.63	0.77	0.7
Software and Hardware Security	0.39	0.78	0.59	0	0.782	0.39	0.79	0.77	0.78
Operational Incident Handling and	0.45	0.7	0.57	0.27	0.717	0.49	0.63	0.64	0.63
Security Measurements	0.21	0.75	0.48	0	0.752	0.38	0.42	0.73	0.58
Cryptology (Cryptography and	0.21	0.71	0.46	0	0.717	0.36	0.42	0.67	0.54
Legal Aspects	0	0.83	0.42	0	0.855	0.43	0	0.74	0.37
Theoretical Foundations	0.08		0.08	0		0	0.16		0.16

1.2.2 ICT Technologies

As shown in Table 3, IoT is the leader in our ranking of ICT Technologies. 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 3: Total ranking for ICT technologies

ICT Technologies	AVERAGE			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Internet of Things	1	0.91	0.96	1	0.908	0.95	1	0.91	0.98
Cloud and Virtualization	0.71	0.88	0.79	1	0.888	0.94	0.42	0.83	0.61
Mobile Devices	0.68	0.89	0.79	1	0.885	0.94	0.37	0.91	0.58
Big Data	0.58	0.87	0.72	1	0.87	0.94	0.16	0.88	0.44
Operating Systems	0.37	0.85	0.61	0.73	0.855	0.79	0	0.79	0.3
Industrial Control Systems	0.3	0.83	0.56	0.38	0.83	0.61	0.21	0.83	0.39
Embedded Systems	0.54		0.54	0.35		0.35	0.74		0.74
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	0.2
Supply Chain	0	0.75	0.37	0	0.74	0.37	0	0.77	0.19
Information Systems	0.36		0.36	0.35		0.35	0.37		0.37

1.2.3 Applications

As shown in Table 4, *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 4: Total ranking for applications

Applications	AVERAGE			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	0.45	0.43	0.81	0.41
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	0.54	0.65	0.65	0.65	0.43	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	0.37	0.73	0.73	0.73	0	0	0
Defense	0		0	0		0	0		0

2 CRITICAL APPLICATIONS 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 desktop analysis (see Table 2). 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.

2.1 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.

For the analysis of the coverage of domain needs by R&I funding programs, we specified the importance of every cybersecurity technology topic for the Maritime domain and compared it with the results of our overall analysis (Table 2) in Table 5.

Table 5: Comparison of R&I priorities in the US and the EU for the Maritime domain

CSP technologies	Importance	US priority	EU priority
Assurance, Audit, and Certification	medium	0.16	1.00
Cryptology (Cryptography and Cryptanalysis)	high	0.42	0.00
Data Security and Privacy	high	0.53	0.73
Education and Training	high	0.47	1.00
Operational Incident Handling and Digital Forensics	medium	0.63	0.27
Human Aspects	medium	0.63	0.38
Identity and Access Management (IAM)	high	0.79	0.35
Security Management and Governance	high	0.79	1.00
Network and Distributed Systems	medium	0.63	0.73
Software and Hardware Security Engineering	high	0.79	0.00
Security Measurements	medium	0.42	0.00
Legal Aspects	medium	0.00	0.00
Theoretical Foundations	low	0.16	0.00
Trust Management, Assurance, and Accountability	high	0.21	0.73

2.2 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.

For the analysis of the coverage of domain needs by R&I funding programs, we specified the importance of every cybersecurity technology topic for the Healthcare domain and compared it with the results of our overall analysis (Table 2) in Table 6.

Table 6: Comparison of R&I priorities in the US and the EU for the Healthcare domain

CSP technologies	Importance	US priority	EU priority
Assurance, Audit, and Certification	medium	0.16	1.00
Cryptology (Cryptography and Cryptanalysis)	high	0.42	0.00
Data Security and Privacy	high	0.53	0.73
Education and Training	high	0.47	1.00
Operational Incident Handling and Digital Forensics	medium	0.63	0.27
Human Aspects	medium	0.63	0.38
Identity and Access Management (IAM)	high	0.79	0.35
Security Management and Governance	high	0.79	1.00
Network and Distributed Systems	medium	0.63	0.73
Software and Hardware Security Engineering	high	0.79	0.00
Security Measurements	medium	0.42	0.00
Legal Aspects	medium	0.00	0.00
Theoretical Foundations	low	0.16	0.00
Trust Management, Assurance, and Accountability	medium	0.21	0.73

2.3 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.

For the analysis of the coverage of domain needs by R&I funding programs, we specified the importance of every cybersecurity technology topic for the Financial domain and compared it with the results of our overall analysis (Table 2) in Table 7.

Table 7: Comparison of R&I priorities in the US and the EU for the Financial domain

CSP technologies	Importance	US priority	EU priority
Assurance, Audit, and Certification	medium	0.16	1.00
Cryptology (Cryptography and Cryptanalysis)	high	0.42	0.00
Data Security and Privacy	high	0.53	0.73

CSP technologies	Importance	US priority	EU priority
Education and Training	high	0.47	1.00
Operational Incident Handling and Digital Forensics	high	0.63	0.27
Human Aspects	medium	0.63	0.38
Identity and Access Management (IAM)	high	0.79	0.35
Security Management and Governance	high	0.79	1.00
Network and Distributed Systems	medium	0.63	0.73
Software and Hardware Security Engineering	high	0.79	0.00
Security Measurements	medium	0.42	0.00
Legal Aspects	medium	0.00	0.00
Theoretical Foundations	low	0.16	0.00
Trust Management, Assurance, and Accountability	high	0.21	0.73

2.4 ICT technology analysis summary

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 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.

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.

Finally, *Legal Aspects* did not get much attention in the EU or in the US, although it has been found to be relatively 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.

3 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.

3.1 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 is 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.*

3.1.1 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.

3.1.2 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.

3.2 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.

3.2.1 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.

3.2.2 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.

3.3 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 fights 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.

3.3.1 Implementation suggestions

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

Government: Increase funding for cybersecurity.

3.3.2 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.

3.4 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.

3.4.1 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.

3.4.2 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[20]) programme with the US National Science Foundation´s US-EU Internet Core & Edge Technologies (ICE-T[21]) initiative.

3.5 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[22]. 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.

3.5.1 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

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

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

[22] 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.

3.5.2 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.

3.6 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.

3.6.1 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.

3.6.2 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.

3.7 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.

3.7.1 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.

3.7.2 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.

3.8 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.

3.8.1 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.

3.8.2 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.

4 CONCLUSIONS

This White Paper 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 White Paper 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.

aegis accelerating EU–US Dialogue in Cybersecurity and Privacy

Quotation:

When quoting information from this report, please use the following phrase: "White Paper on Research and Innovation in Cybersecurity. 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