Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation

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

EXECUTIVE SUMMARY

The report on Cybersecurity and Privacy Research and Innovation (R&I) priorities presents the results of a survey conducted by the AEGIS project in the EU and the US to identify R&I priorities for future collaboration in cybersecurity and privacy between both regions.

The online survey was carried out from 10 May 2018 until 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 Centers (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 varied respondent profiles allow us to gain considerable insights from various players with different priorities in the cybersecurity sector.

Findings from the survey suggest a good outlook for future EU-US collaboration in cybersecurity and privacy R&I. The survey revealed that almost one third of respondents (31,8%) had already participated in EU-US collaborative R&I projects and that the great majority of the respondents that had taken part in collaborative projects consider their previous experience as positive (34%) or very positive (45,5%). Furthermore, 23,3% of the individuals surveyed in EU and the US said they were planning to participate in R&I collaborative projects in topics related to cybersecurity and privacy. Oher 65,1% of respondents said that they may participate in the future.

The report underlines the relevance of common research priorities, application areas and sectors in EU and the US. Regarding research domain priorities, respondents overwhelmingly agreed that "Data Security and Privacy" (80,8%) and "Trust and Privacy" (58,0%) are the most important areas for EU-US cooperation. When it comes to application and technology priorities, participants stated that the "Internet of Things" (71,3%) and "Mobile Devices" (61,9%) are areas of focus. Finally, respondents declared that the Health (75,4%) and Financial Services (68,2%) sectors are of considerable importance and need to be protected by cybersecurity applications, technology and research.

The top priorities connected to cybersecurity and privacy R&I were identified using a ranking system, where 1 was "Not Important" and 4 was "Very Important", as shown in the following table:

Research Domains	Average
Data Security and Privacy	3,75
Trust and Privacy	3,42
Fight Against Cybercrime	3,32
Cybersecurity Education	3,31
Compliance with Information Security, Privacy Policies and Regulations	3,24
Privacy Attitudes and Practices	3,16
Security Management and Governance	3,15
Security Engineering	3,13
Risk Management	3,06
Identity and Access Management	3,09
Information Security Behaviour	3,01
Security Measurements	2,99
Cryptology	2,82
Digital Forensics	2,79

The survey also highlighted what respondents deemed to be the primary barriers to Cybersecurity and Privacy R&I collaboration. The three biggest barriers perceived by respondents were the following:

- Differences in policies and legislation on cybersecurity and privacy between the EU and the US (71,2%)
- Lack of coordination between Funding programs in the EU and the US (59,1%)
- Fragmented cybersecurity field between multiple communities (52,3%)

Thus, adopting measures to eliminate this kind of barriers is critical in order to facilitate and accelerate EU-US collaboration in the priority areas identified in the survey. Based on the findings of the survey, it is clear that stakeholders in EU and the US share priorities in the areas of research domains, applications and technologies and sectors of common interest. Therefore, there is great potential for EU-US collaboration.

1 INTRODUCTION

This report on Cybersecurity and Privacy R&I priorities, Deliverable 3.1, presents the results of the survey carried out by the AEGIS project in the EU and the US to identify cybersecurity and privacy R&I priorities and possible barriers to EU-US collaboration.

The online survey was carried out from 10 May 2018 until 31 May 2018. It was sent to ICT and cybersecurity researchers from academia and the industry, decision makers, government institutions and associations in the EU and the US. The objectives of the survey were the following:

- Measure the potential interest in cooperation EU-US cybersecurity and privacy R&I projects and initiatives.
- Identify priority areas of interest for cybersecurity and privacy R&I cooperation between EU and the US.
- Identify perceived barriers for EU-US collaboration in the field.

The report is divided into three sections: methodology, survey results and conclusions. Section 2 describes the methodology employed by the AEGIS team to construct and carry out the survey. This section also provides information on the taxonomy, published by the European Commission, used to create the survey.

Section 3 presents the results of the survey according to the structure of the survey. The section begins with a description of the respondent profiles, including their professional roles and the type and size of their organizations. It then proceeds to describe respondents' perspectives on cybersecurity research collaboration, including who has participated in EU-US collaborative projects and who plans to participate in the future. Next, we describe cybersecurity and privacy R&I priorities for EU-US collaboration, including research domains, applications and technologies and sector priorities. The section concludes by presenting the results of barriers perceived to EU-US collaboration.

Finally, Section 4 presents the team´s conclusions on the survey results.

2 METHODOLOGY

This section describes the methodological approach to design and conduct the online survey in Europe and the US in order to identify priorities for EU-US collaboration in cybersecurity and privacy R&I. The survey was conducted online from 10 May 2018 to 30 May 2018. INMARK coordinated the process of data collection and information monitoring, supported by the AEGIS partners that performed a personal monitoring of the survey across EU and the US.

2.1 Scope and Sample size

The survey was distributed to more than 1.500 relevant stakeholders in EU and the US that were invited via email to participate in the survey. This convenience sample was selected from the partners' well-vetted databases, which includes ICT and cybersecurity researchers from academia and the industry, decision makers, government institutions and associations.

In addition, the survey was shared on AEGIS and on partners´ social media channels. In total, 130 respondents answered the questionnaire, 105 from EU and 25 from US.

2.2 Selection of priorities

The selection process of cybersecurity related R&I priorities included in the AEGIS survey was performed in five steps:

1. **Identification of topics of common interest for future collaboration in cybersecurity and privacy on the basis of previous work carried out by the consortium members.** In particular, AEGIS benefits from the outcomes of the BIC project and the DISCOVERY project.
2. **Screening of topics of particular interest to EU-US cooperation in cybersecurity and privacy.** This includes the exploration of topics across H2020 Work Programmes for 2018-2020, particularly Secure Societies and ICT, as well as NSF Programs 2018.
3. **Application of the EC Taxonomy, as described in the JRC Technical Report *"European Cyber Security Centres of Expertise Map. Definitions and Taxonomy"*[1].** In an attempt to cluster a discipline as complex and multifaced as cybersecurity, this taxonomy adopts a holistic approach based on three dimensions: cybersecurity and privacy research domains; applications and technologies to apply the cybersecurity research results; and sectors to be protected by cybersecurity applications, technologies and research.
4. **Application of the NIST Taxonomy.** This taxonomy has also been used as a reference in the EC Taxonomy. The NIST Computer Security Resource Centre (CSRC)[2] adopted a multidimensional clustering approach based on six cross-cutting areas: security and privacy specific research domains, technologies to perform research; applications, laws and regulations; type of activities; and business sectors.

[1] JRC Technical Report, European Cyber Security Centres of Expertise Map. Definitions and Taxonomy, Version 3.0, 2017.
[2] Information Technology Laboratory: Computer Security Resource Center. (n.d.). Retrieved from https://csrc.nist.gov/topics

5. **Selection of priority topics.** We used the common EC and NIST Taxonomy domains/sub-domains, applications and technologies, and sectors.

In the following tables we present the selected domains, applications and sectors to **be ranked** by the survey respondents.

Table 1: Research Domains

	RESEARCH DOMAIN	EC Taxonomy Definition
1	Cryptology	Cryptology (Cryptography and Cryptanalysis). Mathematical aspects of cryptology, algorithmic aspects, technical implementation and infrastructural architectures, implementation of cryptanalytic methodologies, techniques and tools.
2	Data Security and Privacy	Security and privacy issues related to data in order to (a) reduce by design privacy and confidentiality risks without impairing data processing purposes or (b) prevent misuse of data after it is accessed by authorized entities.
3	Cybersecurity education	Cybersecurity education is within the learning process of acquiring knowledge, know-how, skills and/or competences necessary to protect network and information systems, their users, and affected persons from cyber threats.
4	Digital Forensics	This domain refers to the theories, techniques, tools and processes for the identification, collection, acquisition and preservation of digital evidence.
5	Privacy attitudes and practices	Within human aspects domain that involve the interplay between ethics, relevant laws, regulations, policies, standards, psychology and the human being within the cyber-security realm.
6	Identity and Access Management	This domain covers authentication, authorization and access control of individuals and smart objects when accessing resources. These concerns may include physical and digital elements of authentication systems and legal aspects related to compliance and law enforcement.
7	Security management and governance	Security Management and Governance domain includes methodologies, processes and tools aimed at the preservation of confidentiality, integrity and availability of information as well as other properties such as authenticity, accountability and non-repudiation.
8	Risk management	
9	Information security behavior	
10	Compliance with information security, privacy policies and regulations	
11	Security Engineering	Security aspects in the software and hardware development lifecycle such as risk and requirements analysis, architecture design, code implementation, validation, verification, testing, deployment and runtime monitoring of operation.
12	Trust and privacy	Security requirements engineering with emphasis on identity, privacy, accountability, and trust.
13	Security Measurements	Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant cyber-security performance-related data.
14	Fight against cybercrime	Legal and ethical aspects related to the misuse of technology, illicit distribution and/or reproduction of material covered by IPR and the enforcement of law related to cybercrime and digital rights.

Table 2: Applications and Technologies

	Applications and Technologies
1	Mobile Devices
2	Operating Systems
3	Big Data
4	Industrial Control Systems
5	Supply Chain
6	Internet of Things
7	Cloud and Virtualization
8	Hardware technology (RFID, chips, sensors, routers, etc.)

Table 3: Sectors

	Sectors to be protected
1	Energy
2	Financial services
3	Health
4	Maritime
5	Transportation (Air transport, Rail transport, Road transport)
6	Public Safety

2.3 Online Questionnaire

The questionnaire (Annex 1) comprises a total of 12 questions structured into the following sections:

1. **Basic Information:** Basic data of respondents (country/region, position, organisation type and number of employees).
2. **Perspectives for Cybersecurity research collaboration**: Previous experience in EU-US collaborative R&I projects; overall assessment of EU-US collaboration in R&I; and interest in future collaboration in cybersecurity and privacy projects.
3. **Priority areas for EU-US cooperation in Cybersecurity and Privacy R&I**: Comprises the list of selected research domains, applications and technologies, and sectors to be ranked by respondents according to their relevance for EU-US cooperation.
4. **Barriers for EU-US Cooperation:** Perceived current barriers and problems for taking part in Cybersecurity and Privacy R&I cooperation projects between Europe and the US.

The questionnaire includes four types of questions:

- Single answer questions: Yes or No answers.
- Multiple choice questions, where respondents may choose from a list of options.
- Rating scale questions, where respondents rank a list of options from 1- not important to 4 – very important.
- Open questions.

Online tool

The questionnaire was based on the online survey platform, Survey Monkey[3]. This tool was chosen because it is easy to use for respondents, fast to collect responses and convenient to analyse the results. It has been proved to be the optimised process of distribution, response collection and visualisation of data analysis.

To protect data privacy and safety, the following actions were carried out to avoid accidental deletion of the data gathered:

- There was only one administrator that could access the questionnaires.
- Backups of responses obtained were performed every week.
- Ensure the security of the database collected in the Survey Monkey account.

[3] About Us: We Power the Curious. (n.d.). Retrieved from https://www.surveymonkey.com/mp/aboutus/

3 SURVEY HIGHLIGHTS

3.1 Respondent Profile

Most of the respondents who completed the survey are researchers (33,3%), followed by consultants (17,1%). Researchers and professors together represent 48,8% of the respondents, while managers, directors and C-level positions made up 30,2%. The survey therefore provides valuable insight from individuals in the research sector and the private sector.

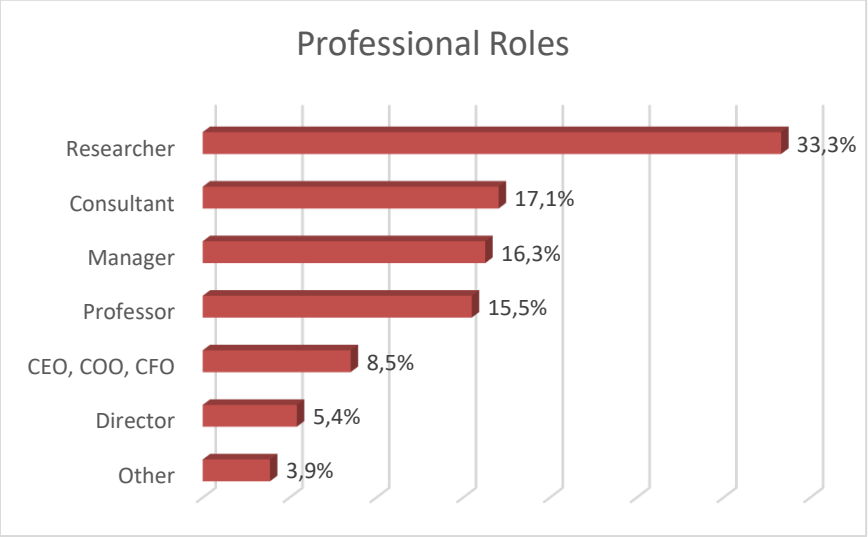


Figure 1 Professional Roles

The survey was completed by individuals in large and small and medium size organizations, including SMEs. Individuals who worked at organizations with more than 250 employees represented the majority of respondents (70,7%). Nonetheless, there was also a significant number of respondents from small and medium-sized organizations, which made up 29,3% of responses, including entities with between 51 – 250 employees (10,8%), 11 – 50 employees (7,7%) and small organizations with less than 10 employees (10,8%).

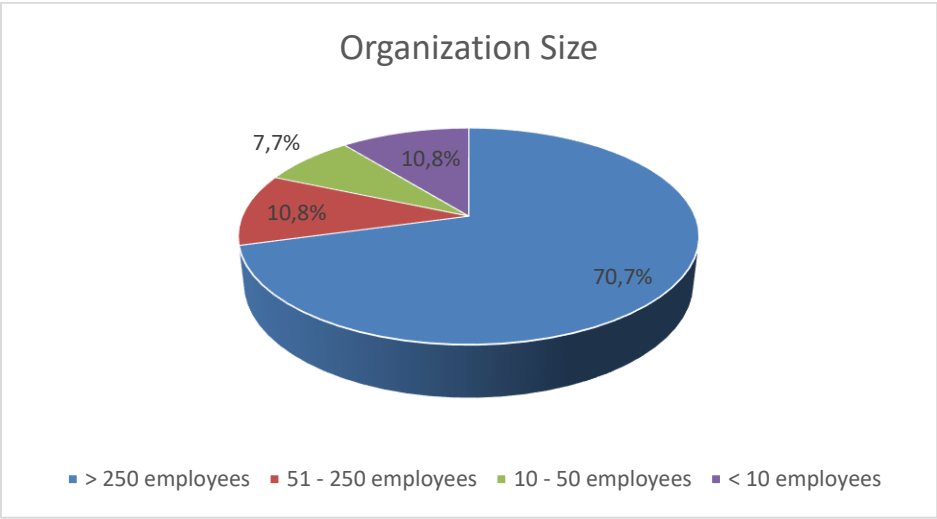


Figure 2 Organization Size

Findings on Respondent Profile

- Respondents in the EU made up 80,8% of the total while respondents in the US made up 19,2%.
- Researchers and professors (48,8%) together with professionals from the private sector (30,2%) represent the vast majority of respondents of the survey on Cybersecurity and privacy R&I priorities.
- Most of the respondents worked at a university (33,3%) or a private company (31,0%). These were followed by individuals who worked at research centers (13,1%).
- Universities and research centers together represent 46,4% of respondents' organisations, followed by private companies (31,0%) and SME (6,8%), and government organizations (6,1%).
- Most of respondents belong to large organisations (70,7%), while 29,3% worked at small and medium size organizations.

3.2 Perspectives for Cybersecurity Research Collaboration

In order to assess the interest in EU-US collaboration on cybersecurity and privacy, respondents were asked about their previous experience in R&I collaboration. Overall, 31,8% of respondents have participated in EU-US collaborative R&I projects. From a regional perspective, there are hardly differences. While in the EU 31,1% of respondents had participated in EU-US collaborative R&I projects, in the US 32,0% of respondents had previous collaboration experience.

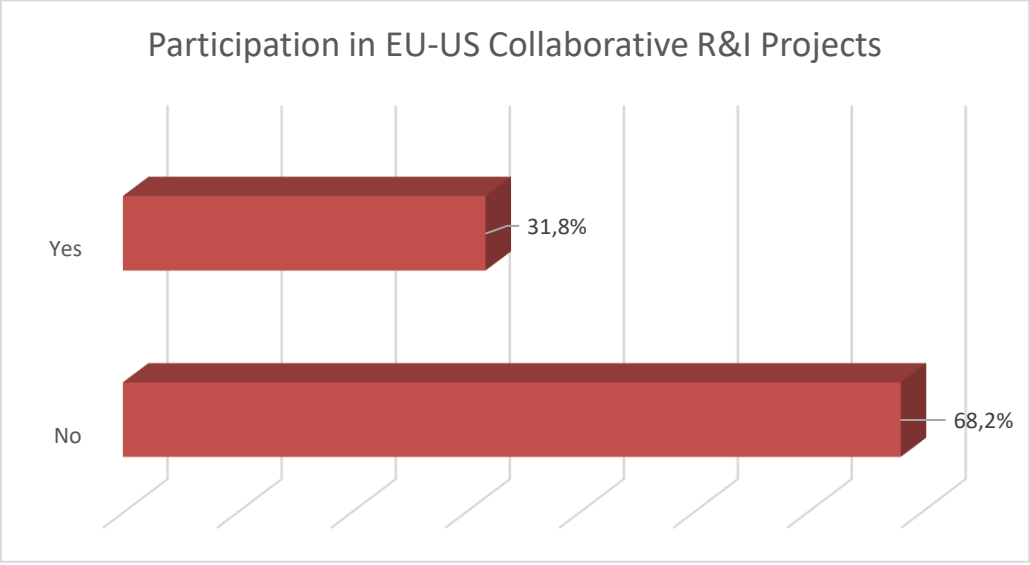


Figure 3: Participation in EU-US Collaborative R&I Projects

Interestingly, 23,3% of all respondents said they were planning to participate in EU-US Cybersecurity and Privacy R&I projects. 65,1% said they maybe would participate in the future and 11,6% declared that they were not planning to become involved in such projects. 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.

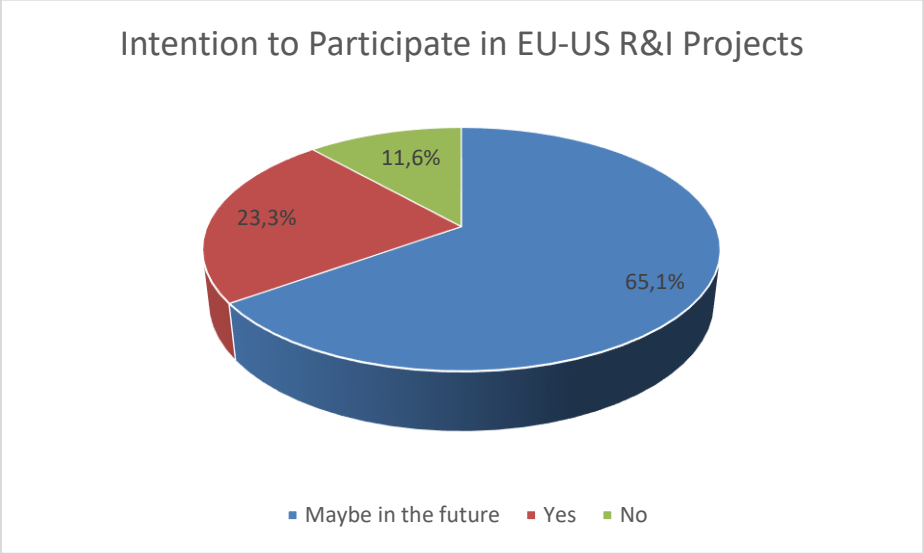


Figure 4: Intention to Participate in EU-US R&I Projects

The intention to participate in EU-US collaborative projects is relatively higher among US respondents. In the EU, 18.8% of respondents declared that they were planning to participate in EU-US R&I collaborative projects, compared to 40,0% in the US. Similarly, 67,9% of EU respondents said they may participate in the future, compared to 56,0% in the US.

In addition to gauging participation, we also believed it was important to analyze respondents´ experience in collaborative projects. Most of those who participated in collaborative transatlantic projects evaluated such experience positively. 45,4% declared their experience had been "Positive" and 34,0% said their experience had been "Very Positive."

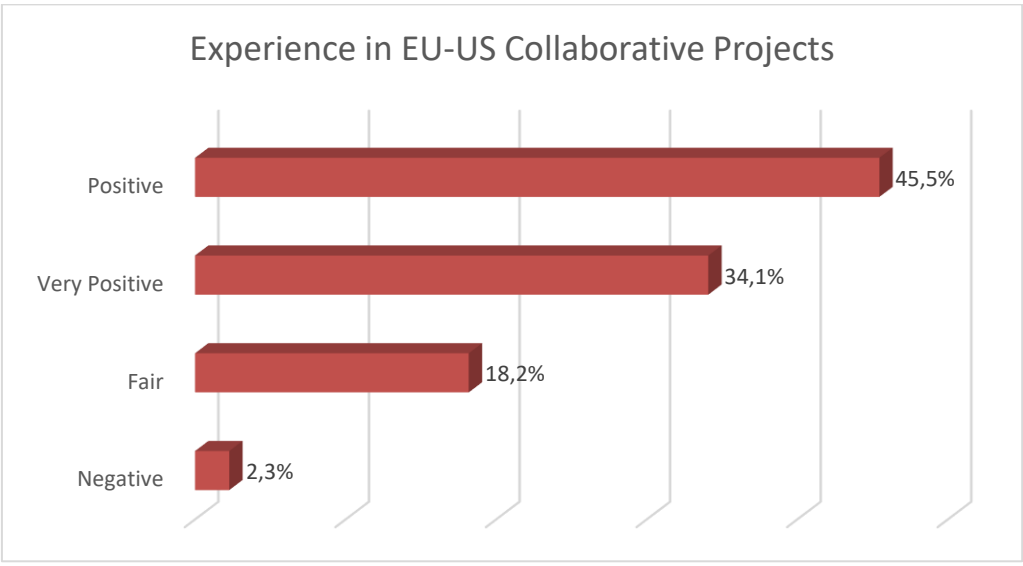


Figure 5: Experience in EU-US Collaborative Projects

Findings on Perspectives for Cybersecurity Research Collaboration

- Almost one third of respondents (31,8%) have previous experience in EU-US collaborative R&I projects.
- The vast majority of respondents that have participated in collaborative projects (almost 80%) have valued their experience as positive or very positive.
- EU participants have a more positive experience in collaborative projects compared with the US. While 81,0% of EU respondents said they had a "Very Positive" or "Positive" experience, roughly 70% of US respondents said they had a "Very Positive" or "Positive" experience.
- H2020 is the most popular funding program among respondents. Of the respondents who had participated in EU-US collaborative projects, 7,7% declared that they had been involved in H2020 projects.
- Of the participants who said they were planning to participate in EU-US Cybersecurity and Privacy R&I projects, 8,5% said they were planning to participate in H2020 projects.

3.3 Priorities for EU-US Collaboration in Cybersecurity and Privacy R&I

Survey respondents were asked to rate the list of research domains, applications and technologies and sectors that were selected on the basis of the common EC and NIST Taxonomy described in section 2. Each topic was scored by respondents according to its importance for EU-US collaboration using a scale of 1 – 4, where 1 is "Not Important" and 4 is "Very Important."

In the following, we analyse the three categories of priorities.

3.3.1 Cybersecurity Research Domains

In terms of **Cybersecurity Research Domains**, the 14 research areas included in the survey are considered important by respondents. As shown in Figure 7, all research domains received a score above average (2,5) and 11 of them were scored above 3 points, which highlights their relevance for EU-US R&I cooperation in Cybersecurity and Privacy.

Data Security and Privacy is the top priority, with a score of 3,75 and 80,8% of respondents considering this research area as very important. It was followed by Trust and Privacy (3,42), Fight Against Cybercrime (3,32) and Cybersecurity Education (3,31), which were rated as very important by more than 50% of respondents.

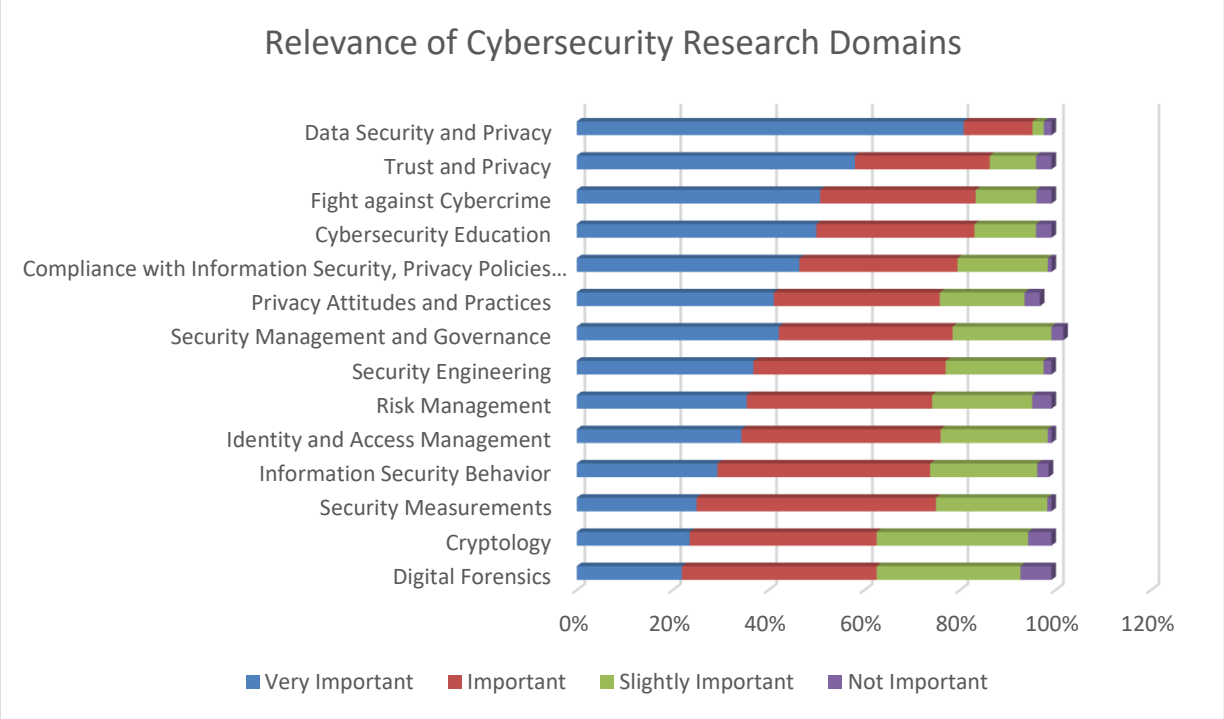


Figure 6: Relevance of Cybersecurity Research Domains

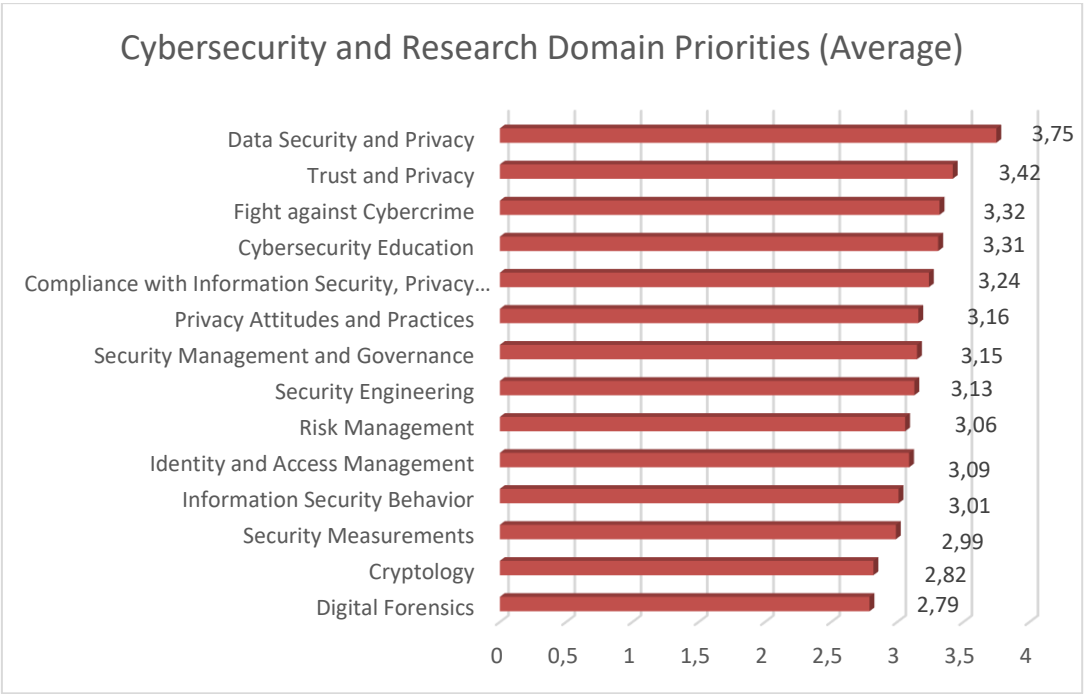


Figure 7: Cybersecurity Research Domain Priorities (Average)

The attached table breaks down research domain priorities by regions. As we can see, there are not many differences when it comes to the top four research domains that survey participants consider the most important. US respondents did break from EU respondents though, declaring Security Management and Governance was one of the most important research areas.

Table 4: Priority Research Domains by Region

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

Findings on Cybersecurity Research Priorities

- Top 4 cybersecurity research priorities for EU-US collaboration are: Data Security and Privacy, Trust and Privacy, Fight Against Cybercrime and Cybersecurity Education.
- Data Security and Privacy, Trust and Privacy and Cybersecurity Education are top priorities shared by EU and US respondents.
- Nonetheless, **in the EU**, the Fight Against Cybercrime is also considered important. It is among the top 4 research priorities in the region.
- **In the US**, Security Management and Government also ranks among the top priorities, taking a spot in the top 4.

3.3.2 Applications and Technologies

In this section of the survey, we asked participants to classify eight **Applications and Technologies** suitable to apply cybersecurity research, according to their importance for EU-US cooperation.

As we saw with research domain priorities, all applications and technologies are of considerable importance for cybersecurity research. All of them received a score above 3 points except supply chain, which was scored 2,98.

Within this context, the results reveal that the most important application area is by far the Internet of Things, with a score of 3,64 and 71,3% of respondents declaring it was "very important." It was followed by Mobile Devices (3,56) and Big Data (3,48) that are considered "very important" for 61,9% and 57,9% of respondents respectively.

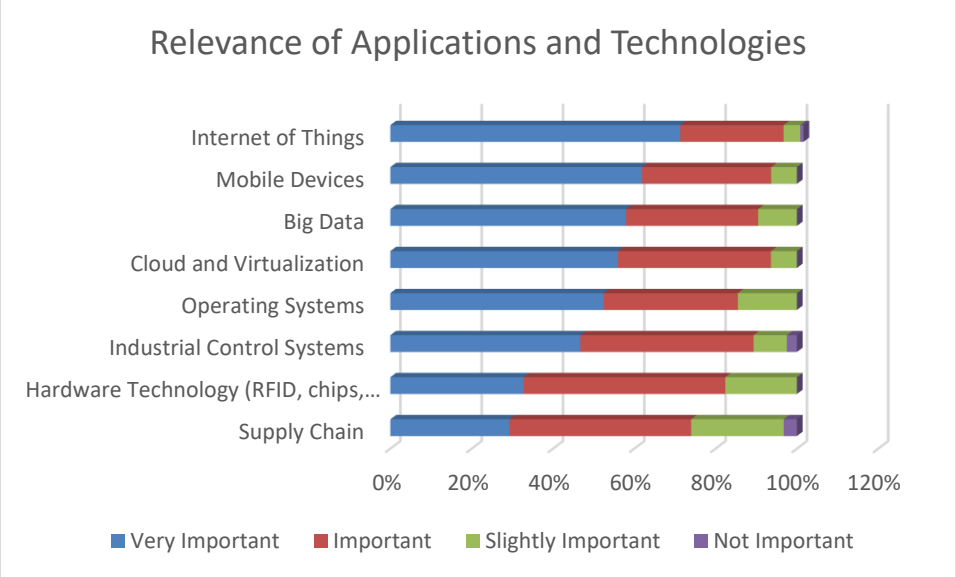


Figure 8: Relevance of Applications and Technologies

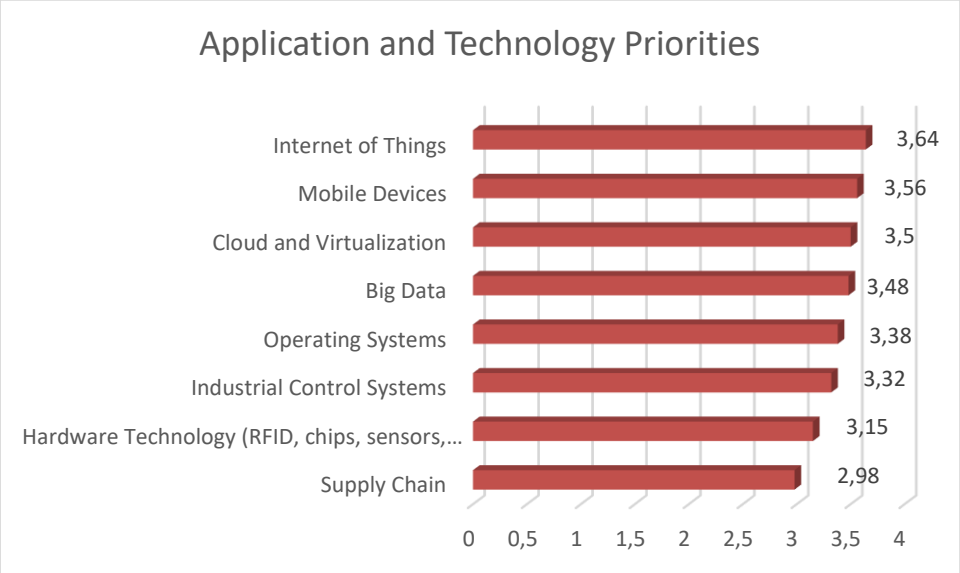


Figure 9: Application and Technology Priorities (Average)

From a regional perspective, the results are very similar. Both EU and US respondents share priorities in the top applications and technologies.

Table 5: Application and Technology Priorities by Region

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

In the following table, we present some connections between applications and technologies and the most relevant research domains. The cross reference of "very important" applications and technologies and research domains shows that cybersecurity research in Data Security and Privacy and Trust and Privacy are considered of particular interest for the selected applications and technologies, i.e. Internet of Things, Mobile Devices, Big Data, Cloud and Virtualization, Operating Systems, Industrial Control Systems, Hardware Technology and Supply Chain. Moreover, research results in the domains of Fight Against Cybercrime and Cybersecurity Education can be applied in most of these applications and technologies.

Table 6: Cross reference between Applications & Research Domains

Applications and Technologies	Research Domains
Internet of Things	• Data Security and Privacy (87,2%) • Trust and Privacy (65,9%) • Fight Against Cybercrime (57,0%)
Mobile Devices	• Data Security and Privacy (85,7%) • Trust and Privacy (66,2%) • Cybersecurity Education (61,8%)
Big Data	• Data Security and Privacy (91,5%) • Trust and Privacy (67,6%) • Fight Against Cybercrime (63,9%)
Cloud and Virtualization	• Data Security and Privacy (91,3%) • Trust and Privacy (71,0%) • Fight Against Cybercrime (61,4%)
Operating Systems	• Data Security and Privacy (87,7%) • Trust and Privacy (64,6%) • Cybersecurity Education (61,5%)
Industrial Control Systems	• Data Security and Privacy (86,0%) • Trust and Privacy (64,9%) • Fight Against Cybercrime (61,4%)
Hardware Technology	• Data Security and Privacy (85,4%) • Trust and Privacy (75,0%) • Compliance with Information Security, Privacy Policies and Regulations (68,3%) • Fight Against Cybercrime (68,3%)
Supply Chain	• Data Security and Privacy (91,7%) • Trust and Privacy (72,2%) • Cybersecurity Education (69,4%)

Findings on Application and Technology Priorities

- Top 4 Application areas for cybersecurity research are Internet of Things, Mobile Devices, Big Data and Cloud and Virtualization.
- The relevance of selected applications areas and technologies for cybersecurity research results is similar in the EU and the US.
- Researchers also identified Operating Systems as one of the most important application areas, just after Internet of Things and Mobile Devices.
- Industry respondents (managers, consultants, CEOS, etc.) classified the Internet of Things, Big Data and Cloud and Virtualization as the top priority areas.
- The most relevant cybersecurity research domains connected to the application areas are Data Security and Privacy, Trust and Privacy, Fight Against Cybercrime and Cybersecurity Education.

3.3.3 Main Sectors

Finally, respondents were asked to identify **relevant Sectors that need to be protected by cybersecurity applications, technologies and research**.

The same pattern identified in the other questions on priorities is also present here. As seen in Figure 11 below, respondents gave a general importance to all of the sectors. Health, Financial Services, Public Safety, Transportation and Energy scored over 3 points. Only the Maritime sector scored lower (2,95).

Health was deemed the most relevant sector, with 75,4% of respondents classifying it as very important. It was followed by the Financial Services sector (68,2%) and the Public Safety sector (64,0%).

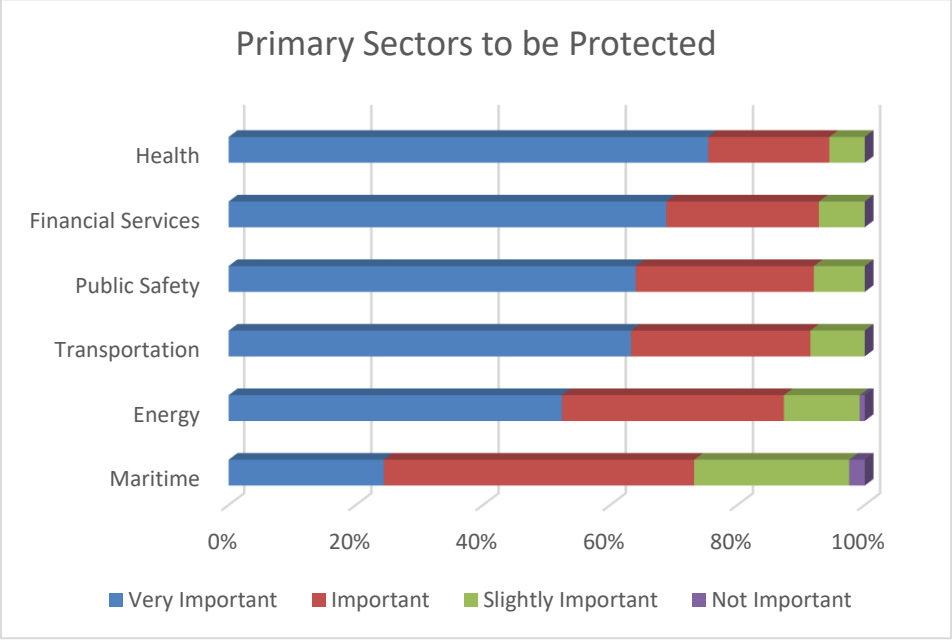


Figure 10: Primary Sectors to be Protected

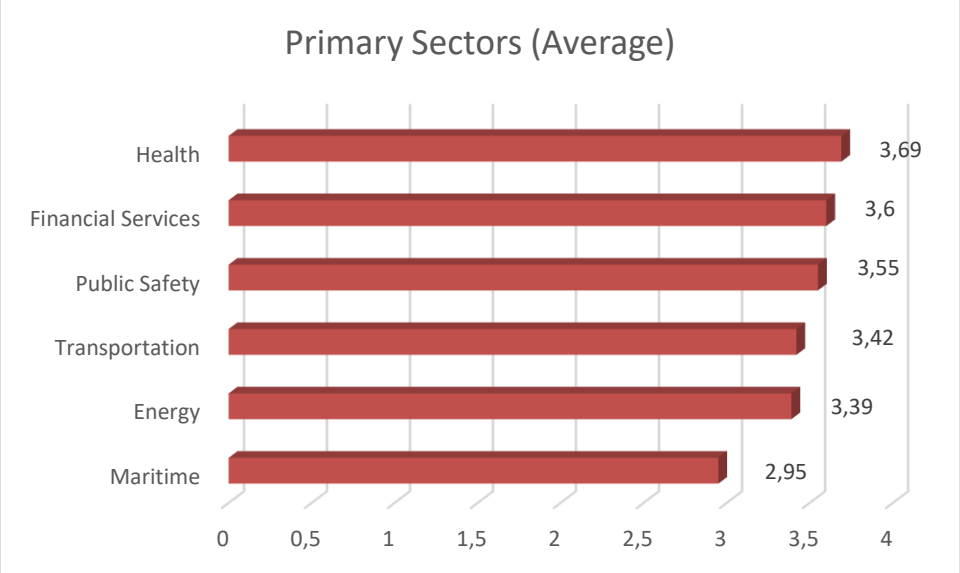


Figure 11: Priority Sectors (Average)

The breakdown of sector priorities by region shows a slight difference when compared to overall results. US respondents give more priority to Health (3,71) and Maritime sector (3,04).

Table 7: Sector Priorities by Region

Sectors	Average	EU	US
Health	3,69	**3,68**	**3,71**
Financial Services	3,60	**3,64**	**3,46**
Public Safety	3,55	**3,62**	**3,25**
Transportation	3,42	**3,45**	**3,38**
Energy	3,39	**3,43**	**3,21**
Maritime	2,95	**2,94**	**3,04**

The table below reflects the cross reference of "very important" sectors and research domains. Like for applications and technologies, there are two research domains, Data Security and Privacy and Trust and Privacy that are considered of particular interest for all selected sectors, i.e. Health, Financial Services, Public Safety, Transportation, Energy and Maritime.

Fight Against Cybercrime is a priority for Financial Services, Public Safety, Transportation and Energy. In addition, Cybersecurity Education is seen of particular relevance for the Health sector, while Compliance with Information Security, Privacy Policies and Regulations is more important for Financial Services and the Maritime sector.

Table 8: Cross Reference between Sectors & Research Domains

Sectors	Research Domains
Health	• Data Security and Privacy (87,1%) • Trust and Privacy (65,2%) • Cybersecurity Education (55,4%)
Financial Services	• Data Security and Privacy (85,9%) • Trust and Privacy (66,7%) • Fight Against Cybercrime (57,0%) • Compliance with Information Security, Privacy Policies and Regulations (57,0%)
Public Safety	• Data Security and Privacy (83,5%) • Trust and Privacy (66,7%) • Fight Against Cybercrime (65,0%)
Transportation	• Data Security and Privacy (87,7%) • Trust and Privacy (68,1%) • Fight Against Cybercrime (66,2%)
Energy	• Data Security and Privacy (86,2%) • Trust and Privacy (65,6%) • Fight Against Cybercrime (63,6%)
Maritime	• Data Security and Privacy (86,2%) • Trust and Privacy (72,4%) • Compliance with Information Security, Privacy Policies and Regulations (70,0%)

Findings on Priority Sectors

- Health, Financial Services and Public Safety are the main priority sectors to be protected by cybersecurity applications, technologies and research.
- In the US, the Maritime sector scored higher (3,01).
- The top priority sectors, Health and Financial Services, have been identified as the most important by researchers as well as by respondents from the private sector (managers, consultants, CEOS, etc.)
- The most relevant cybersecurity research domains connected to key sectors are Data Security and Privacy, Trust and Privacy and Fight Against Cybercrime.

3.4 Barriers for EU-US collaboration in Cybersecurity and privacy R&I

In addition to identifying cybersecurity and privacy priorities, it was also of high importance to single out barriers to EU-US collaboration in these areas. Respondents were asked to select the three main barriers or problems to participate in cybersecurity and privacy R&I cooperation projects from a multiple-choice list.

Responses reflected that the differences in policies and legislation on cybersecurity and privacy between the EU and the US are the biggest barrier (71,2%), followed by the lack of coordination between funding programs in the US and Europe (59,1%) and the fragmented cybersecurity field between multiple communities (52,3%).

Other group of barriers perceived by respondents are the lack of awareness of funding programs in EU/US (39,4%), difficulties to build research and innovation partnerships between the industry and academia (33,3%), rules related to IPR and access rights to background technology and results (27,3%) and the lack of awareness about Cybersecurity and Privacy research topics of common interests (26,5%). Furthermore, differences in terminology on cybersecurity between EU and US was perceived as relatively less important (15,9%).

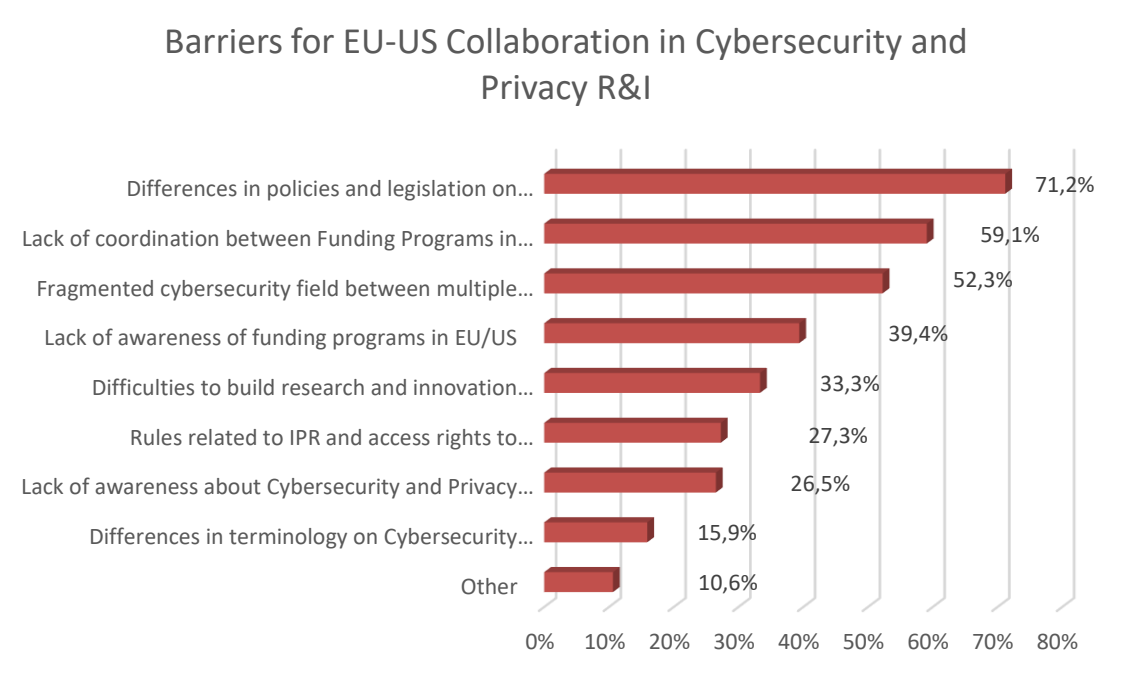


Figure 12: Barriers for EU-US Collaboration in Cybersecurity and Privacy R&I

Additionally, other barriers mentioned in the survey are often related to cultural differences and divergences in research and business approaches. Some of the respondents' comments are included below:

"Lack of regular meeting and networking opportunities where EU and US university researchers have the opportunity to get together for funding proposal collaboration. Additionally, there is a dissimilar model of PhD programs and faculty time available for research in the US and EU. For example, most US faculty teach courses in summer, leaving less time for research compared to their EU counterparts."

"Business orientation and culture differences between both regions."

"Differences in attitude of the public (users) towards privacy issues in the EU and the US."

"Lack of interest in systems of security compared to other domains (e.g., privacy)."

"The greatest problem is the insufficient focus on applied research to provide security at scale."

Findings on Barriers for Cybersecurity and Privacy R&I Collaboration

- Major barriers for EU-US cooperation are the differences in policies and legislation on cybersecurity and privacy between the EU and the US, followed by the lack of coordination between funding programs in the US and Europe and the fragmented cybersecurity field between multiple communities.
- Perceived barriers for collaboration in cybersecurity and privacy R&I are similar in both the EU and the US.
- There are no significant differences among respondents with and without experience in EU-US collaborative projects. The great majority of them perceive the differences in policies and legislation, the lack of coordination between funding programs and the fragmented cybersecurity field as the primary barriers.
- From an industry perspective, the fragmentation of the cybersecurity field in multiple communities is one of the most significant barriers for EU-US collaboration.

4 CONCLUSIONS

Based on the results of the survey conducted among ICT and cybersecurity researchers from academia and the industry, decision makers, government institutions and associations in EU and the US, we have identified priority research domains, application areas and sectors of common interest for EU-US collaboration in cybersecurity and privacy R&I.

These conclusions should not only be taken as important insights, but also as potential points of references to propel EU-US collaborative R&I efforts. It is especially important to highlight the barriers identified by survey respondents and encourage policy makers and key stakeholders from both sides of the Atlantic to take measures to remove some of these roadblocks.

There is an increasing interest in collaborative research and innovation between EU-US in the field of cybersecurity and privacy domains. Almost one third of respondents (31,8%) said that they have been already involved in EU-US collaborative R&I projects, of which 23,3% are planning to participate in new projects or initiatives and 65,1% have interest in participating in the future. This opens good perspectives for future collaboration between the US and EU in 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, among others.

The Top 4 cybersecurity research priorities for EU-US collaboration are Data Security and Privacy, Trust and Privacy, Fight Against Cybercrime and Cybersecurity Education. Among these research domains of common interest for transatlantic collaboration, it is not surprising that **Data security and privacy is seen by more than 80% of the survey respondents as the top research priority in both the US and the EU,** given the policy changes in data security and privacy over the past few years. In fact, the EU implemented what are considered to be the world´s toughest data protection and privacy regulations, the Directive on the Security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR), in May 2018.

The Internet of Things is seen as the top priority application area. "Cybersecuring" the Internet of Things (IoT) is a popular conversation topic lately. There is a general fear within the technology community that IoT devices will be the next big target. As *Wired* noted in an April 2018 article, "Each model of each device is a special snowflake, running inscrutable, proprietary code that makes it difficult to create one-size-fits-all security scanning tools."[4] Our survey respondents confirm this risk and apprehension, with 71,31% of participants declaring that IoT is the most important application area for cybersecurity research results.

Health and Financial Services are overwhelmingly considered the most important sectors to be protected. This finding echoes the focus we have seen from different actors across various industries and organizations. According to CSO[5],

[4] Newman, L. H. (2018, April 16). An elaborate hack shows how much damage IoT bugs can do. Retrieved from https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/

[5] Adefala, L. (2018, March 6). Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries. Retrieved from https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

in the US the healthcare sector is the target of twice as many cyber attacks compared to other sectors, seeing an average of 32.000 intrusion attacks per day in 2017. The financial services sector is also seen a significant sector that must be protected. In its 2017 report, the Financial Stability Board – which is made up of national financial authorities and international standard-setting bodies – highlighted the 2016 cyber attack on the Bangladesh Bank that resulted in the theft of $81 million and the Equifax attack that compromised the financial information of 143 million individuals.[6]

The cybersecurity and privacy community views the different policies and legislation in the EU and the US as a barrier for collaboration. It´s important to note that although the EU and the US share cybersecurity objectives in policy areas such as public-private information sharing and the creation of international or harmonized cybersecurity standards and policies, collaboration between both regions has not always been easy[7]. One example of this is the recent implementation in the EU of the NIS Directive and the GDPR, laws that do not have a US equivalent and which caused some US websites to block access to European visitors because they could not comply with the requisites in time.[8] It´s therefore a logical conclusion that an uneven policy and legislation landscape between both regions can lead to R&I difficulties.

The lack of coordination between funding programs in the US and Europe is also considered an important barrier for R&I collaboration. Previous EU funded projects, such as DISCOVERY, have also identified the lack of coordination between funding agencies as a problem for EU-US collaboration and discussed different ideas for building sustainable mechanisms for future transatlantic collaboration in ICT research. Today it is widely accepted that EU-US collaboration in R&I, including cybersecurity and privacy, will require more effective coordination among funding agencies and thus the involvement of public and private funding with a long-term commitment.

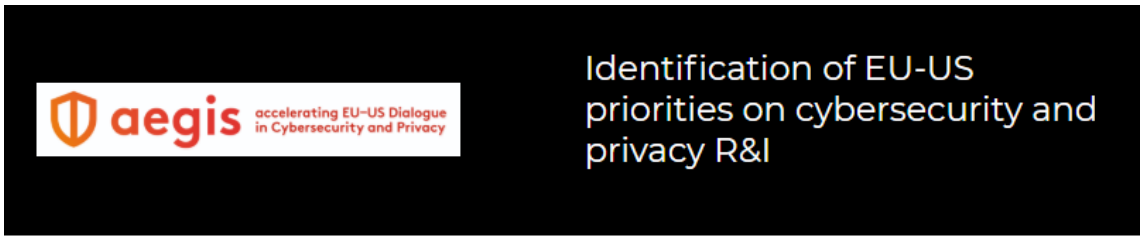
In conclusion, the findings of this survey provide valuable information about potential areas of EU-US collaboration in cybersecurity and privacy R&I and identify the principal barriers for cooperation. It is important that public and private actors take steps to focus their collaboration efforts on areas where there is already shared interest and to eliminate the barriers when possible. The AEGIS project is part of this effort and is working to increase cooperation and dialogue between key EU and US cybersecurity and privacy stakeholders.

[6] Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices. (2017, October 13). Retrieved from http://www.fsb.org/wp-content/uploads/P131017-1.pdf

[7] AEGIS D.1.3 - White Paper on Cybersecurity Policies. Common Ground for EU-US Collaboration, (2018, May 31)

[8] Hern, A., & Belam, M. (2018, May 25). LA Times among US-based news sites blocking EU users due to GDPR. Retrieved from https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times

ANNEX 1 - QUESTIONNAIRE



Welcome to the AEGIS survey!

This survey is being sent out by the AEGIS project, which works to promote cybersecurity and privacy dialogue and cooperation between the US and the EU. Please note that your responses will be kept absolutely confidential and will not be disclosed to any third parties. Data will be used in an aggregated form only and any individual comment will not be attributed to their originators.

Next >>

Basic Information

1. Country: US/EU

- ○ US
- ○ EU

2. What is your position?

- ○ Researcher
- ○ Professor
- ○ Director
- ○ Consultant
- ○ Manager
- ○ CEO, COO, CFO
- ○ Other (please specify)

3. What is your organisation type?

- ○ University
- ○ Research Center
- ○ Private company
- ○ Government organisation
- ○ NGO
- ○ Association
- ○ SME
- ○ Other (please specify)

4. How many employees does your organisation have?

- ○ < 10 employees
- ○ 11 - 50 employees
- ○ 51 - 250 employees
- ○ > 250 employees

Interest in EU-US collaboration on cybersecurity and privacy R&I projects and initiatives

5. Have you participated in EU-US collaborative R&I projects?

- ○ Yes
- ○ No

If yes, please indicate in which topics/areas/Funding Programme

6. If you have already participated in EU-US collaborative projects, what is your overall assessment of such experience (From 1 – Negative to 4 – Very positive)?

- ○ 1- Negative
- ○ 2- Fair
- ○ 3- Positive
- ○ 4- Very positive

7. Are you planning to participate in EU-US Cybersecurity and Privacy R&I projects?

- ○ Yes
- ○ No
- ○ Maybe in the future

If yes, please specify
- In which topic(s)/areas(s)
- The Funding Programme(s)/Grant

Priority areas for EU-US cooperation in Cybersecurity and Privacy R&I

8. **CYBERSECURITY RESEARCH DOMAINS:** Based on your knowledge and experience, please rate (from 1 - Not Relevant to 4 - Very Relevant) the following Cybersecurity and Privacy Research and Innovation priorities according to their relevance for EU-US cooperation.

	1 - Not important	2- Slightly important	3- Important	4- Very important
Cryptology	○	○	○	○
Data Security and Privacy	○	○	○	○
Cybersecurity education	○	○	○	○
Digital Forensics	○	○	○	○
Privacy attitudes and practices	○	○	○	○
Identity and Access Management	○	○	○	○
Risk management	○	○	○	○
Information security behavior	○	○	○	○
Compliance with information security, privacy policies and regulations	○	○	○	○
Security Engineering	○	○	○	○
Security Measurements	○	○	○	○
Trust and privacy	○	○	○	○
Security management and governance	○	○	○	○
Fight against cybercrime	○	○	○	○

9. **APPLICATIONS AND TECHNOLOGIES:** Based on your knowledge and experience, please rate (from 1 - Not Relevant to 4 - Very Relevant) the following Applications and Technologies, on which the cybersecurity research results are applied, according to their relevance for EU-US cooperation.

	1- Not important	2- Slightly important	3- Important	4- Very important
Mobile Devices	○	○	○	○
Operating Systems	○	○	○	○
Big Data	○	○	○	○
Industrial Control Systems	○	○	○	○
Supply Chain	○	○	○	○
Internet of Things	○	○	○	○
Cloud and Virtualization	○	○	○	○
Hardware technology (RFID, chips, sensors, routers, etc.)	○	○	○	○

10. **SECTORS:** Based on your knowledge and experience, please rate (from 1 - Not Relevant to 4 - Very Relevant) the Sectors, which are to be protected by cybersecurity applications, technologies and research, according to their relevance for EU-US cooperation.

	1- Not important	2- Slightly important	3- Important	4- Very important
Energy	○	○	○	○
Financial services	○	○	○	○
Health	○	○	○	○
Maritime	○	○	○	○
Transportation (Air transport, Rail transport, Road transport)	○	○	○	○
Public Safety	○	○	○	○

Barriers for EU-US collaboration

11. What do you think are the main barriers/problems for taking part in Cybersecurity and Privacy R&I cooperation projects between Europe and the US? (Please select the three most important.)

- ☐ Fragmented cybersecurity field between multiple communities
- ☐ Differences in terminology on Cybersecurity between EU and US
- ☐ Differences in policies and legislation on cybersecurity and privacy between EU and US

- [ ] Lack of awareness of funding programs in EU/US
- [ ] Lack of awareness about Cybersecurity and Privacy research topics of common interests
- [ ] Lack of coordination between Funding Programs in the US and Europe
- [ ] Rules related to IPR and access rights to background technology and results
- [ ] Difficulties to build research and innovation partnerships between industry and academia
- [ ] Other (please specify)

12. If you would like to receive the result of the survey, please share your email with us (optional).

End of survey

<< Prev Done

aegis

accelerating EU–US Dialogue in Cybersecurity and Privacy

Quotation:

When quoting information from this report, please use the following phrase:

"Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation. 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