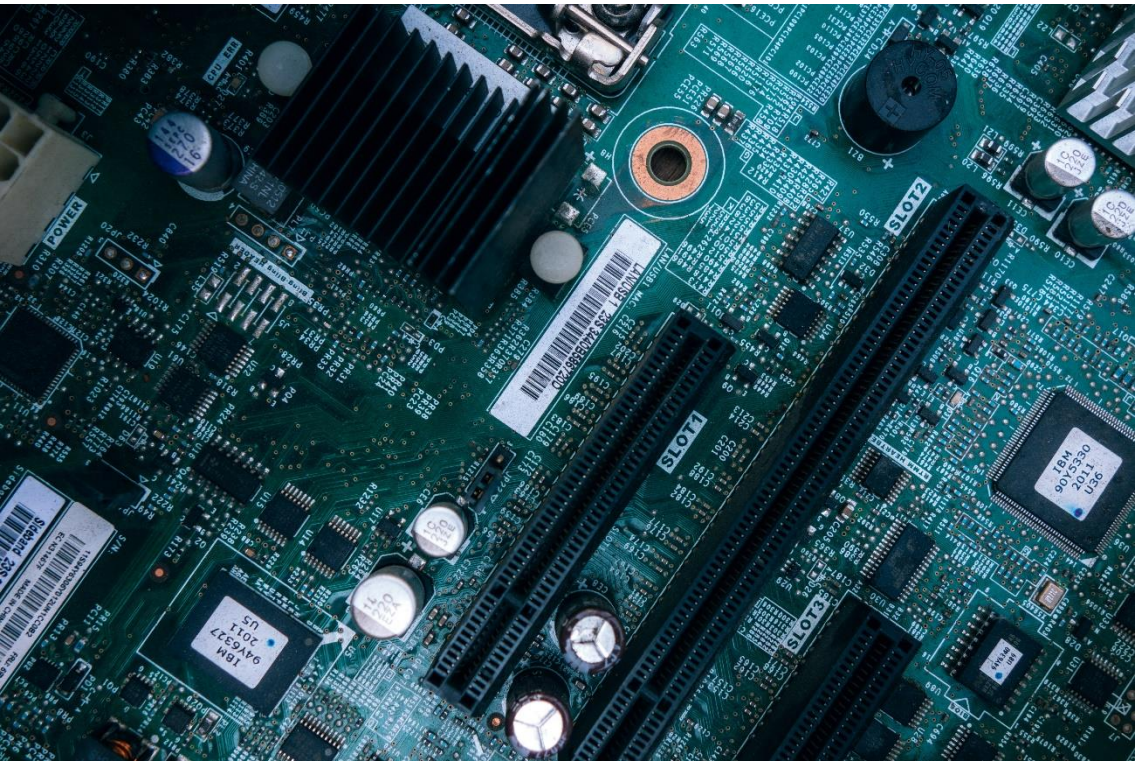
aegis accelerating EU–US Dialogue in Cybersecurity and Privacy



POLICY BRIEF 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

Page

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

It is clear that the development of information technology as well as its rapid penetration and effect on modern industry and society is similar in both the European Union and the United States. It is not surprising, therefore, that cybersecurity and privacy funding programs in both jurisdictions focus on similar areas.

However, for funding program managers, it is important to identify what areas both countries have classified as promising topics and where focus areas diverge. In the latter case, it could signal excessive funding by one side or vice versa.

AEGIS has created this policy brief in order to lay out the current landscape in cybersecurity and privacy R&I in the EU and the US. The policy brief is based on the "White Paper on Research and Innovation in Cybersecurity" developed by the project.

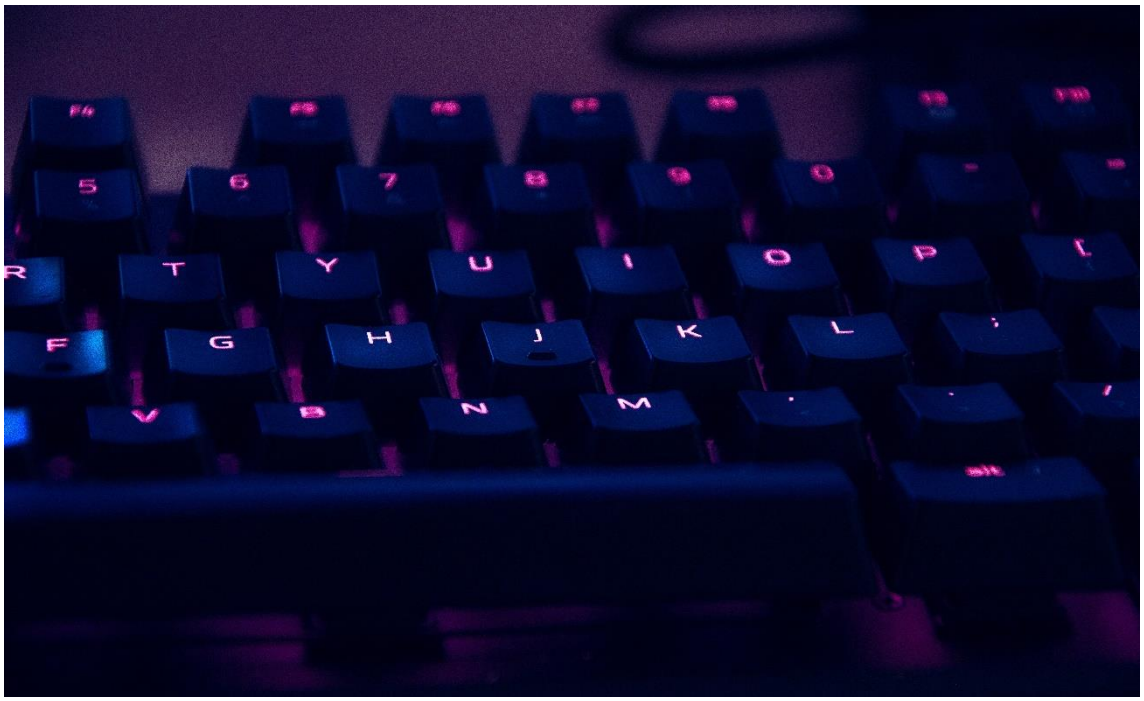
Our key findings are as follows:

- Cybersecurity topics such as *Security Management and Governance; Data Security and Privacy; Education and Training; Assurance, Audit and Certification;* and *Network and Distribution Systems* get the most attention from funding program managers as well as from the research community.

- The *Internet of Things* 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*. Meanwhile, the cybersecurity applications considered to be priorities are *Energy, Public Safety, Transportation, Financial Services* and *Healthcare*.

- When analysing the Healthcare, Financial and Maritime applications domains, we found that most of these domains are classified as highly important priorities and are well covered by available funding programs.

1 INTRODUCTION



Although the cybersecurity and privacy landscapes in the EU and the US are undoubtedly different – which is only natural given the different legal, political, cultural and business factors in each region – there are various areas where their priorities are the similar. When it comes to cybersecurity, it is important to consider these shared priorities when designing and developing transatlantic cooperation efforts.

However, it is also important to consider the differences and analyse whether they represent opportunities for improvement. This policy brief aims to help stakeholders and funding program managers understand the priority areas in cybersecurity and privacy R&I and provide useful recommendations for improvement that will benefit both regions in the future.

The document is organized as follows:

Section 2, "**EU-US priorities for R&I in cybersecurity and privacy**," analyses the cybersecurity priorities established in the EU and the US and the budget to fund those priorities. It also presents a desktop analysis, using the Joint Research Centre taxonomy, of technologies identified in the AEGIS survey on cybersecurity and privacy priorities.

Section 3, "**Critical applications and demand for cybersecurity and privacy**" addresses the critical cybersecurity domains identified by AEGIS – such as the Maritime, Health and Financial domains – and lays out the biggest issues in each area. Despite the high demand for cryptography, AEGIS has found that this area has received little attention from R&I programs.

To conclude, section 4 ("**AEGIS recommendations for EU-US collaboration in cybersecurity and privacy R&I**") presents AEGIS recommendations for EU-US collaboration in cybersecurity and privacy R&I. It also outlines potential implementation measures and the expected impact of the recommendations.

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

In order to gain a better understanding of the cybersecurity and privacy R&I funding programs in the EU and the US, it is important to analyse each country´s stated priorities and initiatives in those areas. The AEGIS consortium has decided to map each country´s priorities against the Joint Research Centre´s taxonomy for cybersecurity.

The JRC´s taxonomy defines three vectors for categorizing CSP (Cybersecurity and Privacy) R&I directions. It is important to note that we use slightly different names for the three vectors, which include:

- Cybersecurity Research Domains;
- Applications and Technologies; and
- Sectors.

We then proceed to qualitatively analyse the attention devoted by the EU and the US to topics relating to cybersecurity and privacy.

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

2.1 Analysis of priorities

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. AEGIS has decided to analyse the following documents and programs to determine US priorities:

U.S. priorities in cybersecurity are shaped by many publications and initiatives. This partly due to the fact that policymaking in the country is a multi-layered process.

- 2016 Report from the President´s Commission on Enhancing National Cybersecurity;
- 2011 Federal Cybersecurity Research and Development Strategic Plan;
- National Science Foundation´s Secure and Trustworthy Cyberspace Program;
- Department of Homeland Security´s Cyber Security Division Program;
- DARPA Programs; and
- IARPA Programs.

Recently, US President Donald Trump released a new National Cybersecurity Strategy, which set new goals and objectives for the advancement of cybersecurity in the country. We acknowledge its importance for the future of US R&I, but we believe that it is too soon to know what effect it will have on cybersecurity related programs.

Based on these documents, we can come to the following conclusions. As shown in Table 1 and Figure 1, DARPA and the US Department of Defense invest more in cybersecurity, which is understandable since both agencies are military driven. It is not possible to analyse more details of the Department of Defense´s funding programs, as they are not published for the general public. However, DARPA´s funded programs are available for reference on its website.

Table 1: US budget for R&I programs 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

Since the National Science Foundation and the Department of Homeland Security make significant investments in cybersecurity and privacy R&I and have detailed research funding programs publicly available, they have been included in our analysis.

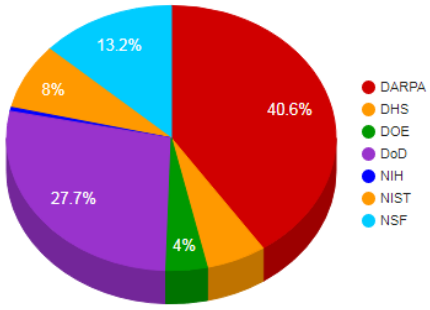


Figure 1: 2018 Cybersecurity budget distribution for US agencies

EU

Compared to the US, the EU´s policies and initiatives on cybersecurity have been limited to concrete actions (versus a variety of publications and programs). AEGIS analysed several key EU initiatives, listed below, to develop its analysis. These efforts have been selected in order to obtain a better understanding of the R&I priorities in cybersecurity and privacy as well as on the basis of their influence in Europe. It is worth noting that AEGIS partners play a significant role in a majority of the initiatives.

- Horizon 2020 R&I Funding Program;
- Contractual Public Private Partnership (cPPP) in Cybersecurity;
- European Cyber Security Organisation Initiative;
- European Union Agency for Network and Information Security; and
- The Network and Information Security Platform Initiative;

In terms of funding for cybersecurity and privacy priorities, it is important to highlight the role of the Horizon 2020 program for R&I. Horizon 2020 is the largest European R&I funding program and without a doubt the most significant. It has an €80 billion, seven-year budget and will be available from 2014 to 2020. As a guiding principal,

H2020 aims to increase the number of breakthroughs and discoveries by helping take ideas from the research lab to the market.

H2020 addresses cybersecurity in its project scope. 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 the European digital economy and encourages European industry players to comply with the current EU regulations and directives, such as the NIS Directive, eIDAS and GDPR.

2.2 Unified analysis with 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[1] 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[2].

In order to determine overall priorities (i.e., the total score) in 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 normalized to get the values in the interval [0;1]).

In this section, we aggregate the results of the desktop analysis and survey using the JRC Taxonomy. We take quantitative values obtained in the desktop analysis and the normalized results (or those divided by 4, i.e., the maximum value) of the AEGIS priorities survey and find the average. In the cases where our survey did not consider some topics, the corresponding cells are left blank and only the value of the desktop analysis is propagated. All the final tables are sorted by the total average value.

Table 2: Total ranking for cybersecurity technologies

Cybersecurity Technology	AVERAGE			EU			US		
Categories	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Security Management and Governance	0.89	0.79	0.84	1	0.79	0.9	0.79	0.78	0.79
Data Security and Privacy	0.63	0.94	0.78	0.73	0.94	0.84	0.53	0.94	0.73
Education and Training	0.74	0.83	0.78	1	0.84	0.92	0.47	0.79	0.63
Assurance, Audit, and Certification	0.58	0.81	0.69	1	0.83	0.92	0.16	0.75	0.45
Network and Distributed Systems	0.68		0.68	0.73		0.73	0.63		0.63

[1] 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.
[2] 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/

Identity and Access Management	0.57	0.77	0.67	0.35	0.78	0.56	0.79	0.75	0.77
Trust Management, Assurance, and Accountability	0.47	0.86	0.66	0.73	0.93	0.83	0.21	0.82	0.52
Human Aspects	0.51	0.79	0.65	0.38	0.79	0.59	0.63	0.77	0.7
Software and Hardware Security Engineering	0.39	0.78	0.59	0	0.78	0.39	0.79	0.77	0.78
Operational Incident Handling and Digital Forensics	0.45	0.7	0.57	0.27	0.71	0.49	0.63	0.64	0.63
Security Measurements	0.21	0.75	0.48	0	0.75	0.38	0.42	0.73	0.58
Cryptology (Cryptography and Cryptanalysis)	0.21	0.71	0.46	0	0.71	0.36	0.42	0.67	0.54
Legal Aspects	0	0.83	0.42	0	0.85	0.43	0	0.74	0.37
Theoretical Foundations	0.08		0.08	0		0	0.16		0.16

2.2.1 Cybersecurity technologies

As shown in Table 2, the analysis of cybersecurity technologies topics demonstrates that *Security Management and Governance* is the area that receives the highest priority. It is closely followed by *Data Security and Privacy* and *Education and Training*.

In the results, *Cryptography* gets quite a quite a low score in the EU and the US. The *Legal Aspects* topic also gets low scores, regardless of the high scores it received in the survey (where it is referred to as the "Fight Against Cybercrime").

There are some key differences in the priority topics in 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 is seen for the *Assurance, Audit and Certification* and *Trust Management, Assurance and Accountability* topics, where the EU scores are higher than the US scores. We see that these results are primarily driven by the values from the desktop analysis. The results of the survey, meanwhile, do not differ much.

2.2.2 ICT technologies

Table 3: Total ranking for ICT technologies

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

As shown in Table 3, an analysis of ICT technologies demonstrates that IoT is the leading priority topic. However, it is important to point out that there is not much difference in the first four ranked positions in the EU. This is because *Cloud and Virtualization*, *Mobile Devices* and *Big Data* are separated by small differences. Meanwhile, *Operating Systems,* the next topic in the ranking, features scores that are quite behind.

It is important to note that *Embedded Systems* and *Critical Infrastructures* have very high scores in the US, but low scores in the EU.

2.2.3 Applications

Table 4: Total ranking for applications

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

Energy is the application domain that is considered the highest priority, as can be seen in Table 4. It is followed by *Public Safety* and *Transportation*. Moreover, we would like note that in the US, it is probable that *Transportation* received a low score because it could be considered part of *Embedded Systems* (such as ICT Technology, for instance, which has very high scores in the US). *Public Safety, Financial Services* and *Healthcare* also have low scores in the US (particularly in the desktop analysis).

Finally, we can observe that *Supply Chain* receives a high score in the US and a low score in the EU. The topic was not investigated in our survey and we cannot confirm the findings.

3 CRITICAL APPLICATIONS AND DEMAND FOR CYBERSECURITY AND PRIVACY

AEGIS has selected several application domains for analysis in order to determine whether the prioritized 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 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.

Table 5: Coverage for Maritime, Healthcare and Financial application domains

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

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

3.1 Maritime

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

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

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

AEGIS proposes the following topics and actions for EU-US collaboration on Maritime.

Table 6: Topics and actions for EU-US collaboration in the Maritime domain

Topics	Actions
• Cybersecurity framework for complex maritime ICT environment (cyber risk management) • Traffic control relying on IoT technology • International (and Inter-institutional) approaches to incident resolution and monitoring • Security system assessment • Innovative cybersecurity training techniques • Deterrence and Collective Defence	• Establish a Crisis Management Centre to organize collective defence and deterrence activities among civil maritime stakeholders • Establish Public-Private- Partnerships for maritime cybersecurity • Develop a cybersecurity "Attribution" program • Improve cybersecurity' skills and capabilities to protect maritime critical infrastructure

3.2 Healthcare

The Healthcare domain includes several sectors to provide goods and services to treat patients. This domain, which includes the hospital, medical and pharmaceutical industries, as well as patients, is exposed a new wide surface of cyber attacks 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 the home, it is possible to connect to a hospital network and connect devices to share data with medical staff. The entire healthcare sector, including device vendors, needs to think proactively about how to keep their devices and their patients safe without compromising clinical functionality.

AEGIS proposes the following topics and actions for EU-US collaboration on Healthcare.

Table 7: Topics and actions for EU-US collaboration in the Healthcare domain

Topics	Actions
• Health data exchange and privacy aspects (including data usage control) • Cybersecurity conformity assessment model • Supply chain assurance model • Innovative cybersecurity training techniques • Securing legacy and new systems (security by design) • Safety/security issues (like diagnostic invasive tools, robots)	• Devote more resources to healthcare R&I projects that provide innovative methods for cybersecurity education and awareness raising • Provide a framework for conformity security assessment at international level • Harmonize standards and legislations for cybersecurity of medical devices and software

3.3 Financial

The financial domain is very appealing for cyber attackers because there is money at stake. The liquid cryptocurrency market is also attractive.

When considering cybersecurity for the financial sector, it is important to consider the security of the user in areas such as online banking. These financial services establish the individual as the end user, who is left to operate alone and must protect himself. This causes problems for the user and the financial institution. For instance, malware installed in a user´s computer could also infect the financial institution.

AEGIS proposes the following topics and actions for EU-US collaboration on Financial services.

Table 8: Topics and actions for EU-US collaboration in the Financial domain

Topics	Actions
• Fighting fake news • Cybersecurity assurance, certification and responsibility • Cyber Insurance • Data security and privacy • Security of new distributed business models: DLT (e.g. Blockchain)	• Agree and prioritize on finance certifications, standards and cyber security regulations • Support R&I projects aiming for complex and distributing crisis management actions • Foster cyber insurance policies in order to increase welfare of society and increase cybersecurity preparedness • Encourage information sharing between governmental agencies at national and international levels

3.1 Privacy

Privacy and security are usually treated together as they are very similar in many aspects and achieving privacy often means installation of security countermeasures. JRC taxonomy is not an exclusion in this case (as well as other, e.g., RSA of NIS WG3) and does not allow singling out privacy only issues, most of which are treated under the umbrella of Data Security and Privacy technology (rated as one of three

top technologies for research in our analysis). AEGIS proposes the following topics and actions for EU-US collaboration on privacy.

Table 9: Topics and actions for EU-US collaboration in privacy

Topics	Actions
• Privacy Risks Management Framework • Privacy Enhanced Technologies (PET) • Privacy by design • Partial identities	• Invest in development of Privacy Risk Management Framework for Europe. • Support analysis of requirements of end users for PET. • Study incentives for usage of PET and ways to foster these incentives. • Raise privacy awareness among citizens.

3.2 Overall ICT technology analysis

In addition to studying the focus areas identified by our team, the AEGIS team also carried out an analysis on ICT technology in general. We found that in most cases, cybersecurity technologies are well covered by existing R&I programs. There are only a few areas that require specific attention.

First, we would like to underline the striking difference between the high demand for cryptography in many domains and the lack of attention it receives from R&I funding programs in 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.

The *Assurance, Audit and Certification* area, which is consider high priority in the EU, is not covered well 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 legislation. Meanwhile, the *Software and Hardware Security Engineering* area receives little attention in the EU but is considered high priority in the US. This area is important and relevant for many application domains. The EU may be able to gain more knowledge in this area by collaborating with the US.

On a final note, the *Legal Aspects* area did not get much attention in the EU or the US, although it is an area considered 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 programs. Although this may be true, it is important to consider the technological aspect in order to formulate the best laws and ensure reliable law enforcement.

4 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 techniques to prevent cybercrimes. AEGIS presents the following recommendations and implementation suggestions to help foment this cooperation.

Recommendation	Implementation Suggestions	Expected Impact
Establish areas for collaboration that interest both the EU and the US.	Develop specific programs within the usual CSP R&I funding programs and others on mutual interest areas.	• EU-US knowledge exchange and projects • Strengthened EU-US relationships.
Take an international approach to cybersecurity.	Increase efforts to counter cross-border cybercrime. Establish cross-program calls for R&I projects on countering international cybercrime.	• Strengthened relationships between crime fighting agencies in both jurisdictions. • Reduced number of cybercrimes.
Invest in international cybersecurity projects.	Increase funding for cybersecurity. Redirect or allocate money.	• Increased interest in EU-US CSP collaboration. • Better relationships between EU-US R&I entities.
Establish or improve international coordination between funding programs.	Find and establish contacts with transatlantic funding agencies. Organize collaborative programs. Specify funding procedures and rules for collaboration.	• Establishment of collaborations between different funding programs. • Exchange of best practices for running programs.
Reduce legislative barriers for cybersecurity and privacy collaboration.	Harmonize legislation requirement frameworks. Cooperate with other research funding programs in other countries to establish basic rules for international projects.	• Establishment of relaxed legal approaches for collaborative research. • Increase in the number of collaborative research projects.
Promote cybersecurity information sharing.	Encourage information sharing between governmental agencies at all levels. Support research of information sharing schemas.	• Increase in information sharing and data pools. • Increase in CSP R&I due to availability of data. • More effective CSP solutions.
Invest in cybersecurity education and training.	Devote more attention to support for cybersecurity education and training. Create EU-US programs for education and training.	• Increased number of events with foreign participants and lecturers. • Elevated level of education in both regions.
Support securing Critical Infrastructure.	Establish programs for EU-US projects in specific fields and encourage information sharing in these sectors.	• More international projects on Critical Infrastructure. • Increased number of solutions for Critical Infrastructure problems.

aegis

accelerating EU–US Dialogue in Cybersecurity and Privacy

Quotation:

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