Part II: Technology Perspective

Chapter 8. Cybersecurity and privacy

List of Authors: Jim Clarke, Fabio Martinelli, Artsiom Yautsiukhin, Claudio Caimi, Alberto Terzi, Silviya Nonova, Camille Sailer, Jody Serrano, Yolanda Ursa

Author affiliation: AEGIS (Accelerating EU-US Dialogue for Research and Innovation in Cybersecurity and Privacy) Consortium. Horizon 2020 Framework Programme.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF ABBREVIATIONS

CISA Act	Cybersecurity and Infrastructure Security Agency
CISA	Cybersecurity Information Sharing Act
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
cPPP	Contractual Public-Private Partnership
CSD	Cyber Security Division
CSDP	Common Security and Defense Policy
CSIRT	Computer Security Incident Response Team
DARPA	Defense Advanced Research Projects Agency
DHS	Department Homeland Security
E-Sign Act	Electronic Signatures in Global and National Commerce Act
ECSO	European Cyber Security Organization
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
H2020	Horizon 2020 Research & Innovation Program
JRC	European Joint Research Centre
NIS Directive	Directive on Security of Network and Information Systems
NIS Platform	NIS Public Private Platform
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development Program
NSF	National Science Foundation
NPRS	National Privacy Research Strategy
NSTC	National Science and Technology Council
OSTP	Office of Science and Technology Policy
SaTC	Secure and Trustworthy Cyberspace Program
UETA	Uniform Electronic Transactions Act

1 INTRODUCTION

In our increasingly connected world, cybersecurity and privacy have become center stage issues[1]. However, because of the connected nature of the world provided by the Internet and digital technologies, these issues cannot be tackled by one player alone.

The European Union (EU) and the United States (US) are the two regions at the forefront of these cyber challenges. Not only do these jurisdictions account for more than 50% of unique IP addresses on an international level, they are also two economic powerhouses that play a major role in the world's financial wellbeing. This in mind, it goes without saying that the cybersecurity and privacy landscapes and Research and Innovation (R&I) priorities in these regions can significantly influence how these issues are tackled in other countries. The same can be said for the policies adopted by the EU and the US to deal with challenges in these areas, which critically affect business, academia and government relations.

The following chapter will present the key elements of the cybersecurity and privacy landscapes in the EU and the US. It will also highlight each region's R&I priorities, which provide an early look at the future of these areas. Nonetheless, understanding how the EU and the US view cybersecurity and privacy not only requires analyzing the institutions and programs that act to regulate these issues, it also requires analyzing the policies they have adopted to deal with challenges. For this reason, we will also compare and contrast key laws and regulations on both sides of the Atlantic in areas such as standards and certification; data protection and privacy; and public-private information sharing. The chapter will conclude with a series of recommendations that aim to foster cooperation between the EU and the US to advance common cybersecurity and privacy priorities.

[1] This chapter has been prepared by the AEGIS consortium, a Horizon 2020 project which worked to accelerate cooperation between the EU and the US in cybersecurity and privacy R&I.

2 LANDSCAPE OF CYBERSECURITY IN EUROPE AND THE US

2.1 EU Cybersecurity and Privacy Strategy

The EU outlined its cybersecurity strategy in 2013, titling it “An Open, Safe and Secure Cyberspace [6].” The document summarized the EU´s five strategic priorities and actions in the short and long term and laid out how it would achieve these goals. The priorities are as follows:

- Achieve cyber resilience;

- Drastically reduce cybercrime;

- Develop a cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP);

- Develop the industrial and technological resources for cybersecurity; and

- Establish a coherent international cyberspace policy for the European Union that promoted core EU values.

The next sections will outline a number of additional tactical directives and activities carried out in Europe as part of its cybersecurity strategy.

2.2 NIS Public Private Platform (NIS Platform)

The NIS Public-Private Platform was established as part of the EU cybersecurity strategy. It aims to foster the resilience of the networks and information systems, which underpin the services provided by market operators and public administrations in Europe. At the initial scoping meeting in 2013, the NIS Platform was designed into three distinct working groups in order to implement the measures set out in the NIS Directive and to ensure its convergent and harmonized application across the EU.

The main goals of the NIS Platform were to help public and private organizations improve cybersecurity risk management and information sharing, and to prepare a Strategic Research Agenda for secure ICT. A key focus was on turning research results into commercial products to serve Europe's growth and jobs objectives.

CPPP

Within the Digital Single Market Strategy, the European Commission has established a contractual Public-Private Partnership (cPPP) on cybersecurity in order to strengthen the EU's cybersecurity industry. The objective of the cPPP is to stimulate the European cybersecurity sector. This is considered to be a strategic priority within the EU and is being pursued through several actions, including:

- Bringing together industrial and public resources to improve European industrial policy on cybersecurity, specifically on innovation in this field, and following a jointly agreed strategic research and an innovative path;

- Promoting trust between Member States and industrial actors by fostering bottom-up cooperation for Research and Innovation;

- Helping stimulate the cybersecurity industry by aligning the demand and supply of products and services and allowing the sector to efficiently address the future needs of end users;

- Using funding from Horizon 2020 (H2020) and maximizing the impact of available sector funds through better coordination and a better focus on certain technical priorities; and

- Improving the visibility of European excellence in Research and Innovation in cybersecurity and digital privacy.

The public contribution of the cPPP is provided by the European Commission, while the private part is provided by a fully self-financed non-profit organization under the Belgian law called the European Cyber Security Organization (ECSO) [9].

The vastness and complexity of the issues related to cybersecurity require forms of cooperation between entities that, although with different roles, operate in this sector, which is essential for the security and the economy of the European Union. In order to achieve a more effective management, it is necessary to develop every possible synergy that facilitates these integrations and, in this context, ECSO represents a strategic element of great importance.

EU Global Strategy for Foreign and Security Policy

The EU Global Strategy for Foreign and Security Policy adopted in June 2016 increases the bloc´s focus on cybersecurity and supports multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of information. It enhances the EU´s cybersecurity cooperation efforts with core partners such as the US and NATO. In the strategy, the EU states that its security measures will be based on strong public-private partnerships and other measures, such as cooperation and information-sharing between Member States, institutions, the private sector and civil society. These actions can foster a common cybersecurity culture, and increase preparedness for possible cyber disruptions and attacks.

European Agenda on Security

The new European Agenda on Security 2015-2020 gives renewed emphasis to the implementation of existing policies on cybersecurity and addresses new threats and threats that are more international, cross border and cross-sectorial, with cybercrime as one of the three top priorities. Terrorism and organized crime are also considered top priorities.

Digital Single Market Strategy

Finally, the Digital Single Market Strategy is also an important aspect of Europe´s cybersecurity strategy. It includes a contractual public-private partnership on cybersecurity to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, trust between Member States and industrial actors and alignment of the supply and demand for cybersecurity products and solutions.

US cybersecurity and privacy strategy

The current US cybersecurity strategy focuses on four well-defined strategic pillars[2]:

- Protect the homeland, the American people and the American way of life;
- Promote American prosperity;
- Preserve peace through strength; and
- Advance American influence.

Each of these pillars is clearly outlined by US President Donald Trump in the "National Security Strategy," which provides some high-level lines of action and describes the main objectives of the strategy, including the role of the Internet and information technology as a relevant element from a defensive perspective. The first three pillars are particularly focused on cybersecurity issues. The National Security Strategy clearly reflects the US government´s belief that cyberspace is now a fundamental part of every aspect of national security.

Another crucial objective of the new US strategy also includes specific focus areas, such as protection and resilience of national critical infrastructures from cyberattacks. In order to accomplish, the US has decided to dedicate attention to real risks, which cover the following critical areas of intervention: national security, energy, banking and finance, health and safety, communications and transport. The main purpose is to identify where and how cyberattacks could occur and ensure high priority interventions in these areas in terms of support, capacity building, and defense.

[2] https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-announces-national-security-strategy-advance-americas-interests/

The US cybersecurity strategy can be broken into the national federal strategy and an international strategy, although the latter has a relatively small number of instruments (e.g. Strategic Plans).

2.2.1 Federal Cybersecurity Research and Development Strategic Plan

The National Science and Technology Council's (NSTC[3])'s Federal Cybersecurity Research and Development Strategic Plan responds to Section 201 of the Cybersecurity Enhancement Act of 2014, which directs the NSTC and the Networking and Information Technology Research and Development (NITRD[4]) Program to develop a strategic plan to guide federal cybersecurity research and development.

Before going into detail about the strategic plan itself, we will outline the different stakeholders involved in the plan.

- The **NSTC** is the principal entity by which the US government coordinates science and technology policy across the diverse entities that make up the federal research and development (R&D) enterprise. One of the NSTC's primary objectives is establishing clear national goals for federal science and technology investments.
- The **Office of Science and Technology Policy (OSTP)** advises the US president in policy formulation and budget development on questions in which science and technology are important elements; articulates the president's science and technology policy and programs; and fosters strong partnerships among federal, state and local governments as well as in the scientific communities in industry and academia.
- The **Subcommittee on Networking and Information Technology Research and Development** is a body under the Committee on Technology of the NSTC. The NITRD Subcommittee coordinates multi-agency research and development programs to help assure continued US leadership in networking and information technology, satisfy the needs of the

[3] https://www.whitehouse.gov/ostp/nstc/

[4] https://www.nitrd.gov/

federal government for advanced networking and information technology and accelerate development and deployment of advanced networking and information technology.

The Federal Cybersecurity Research and Development Strategic Plan (2016) updates and expands the December 2011 plan, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, which defined a set of interrelated breakthrough objectives for federal agencies that conduct or sponsor R&D in cybersecurity. This plan incorporates and expands the priorities in the 2011 plan and adds a strong focus on evidence-validated R&D. Evidence of cybersecurity efficacy and efficiency, such as formal proofs and empirical measurements, drives progress in cybersecurity R&D and improves cybersecurity practice.

The plan is built on four assumptions:

- **Adversaries**. Adversaries will perform malicious cyber activities as long as they perceive that the potential results outweigh the likely effort and possible consequences for themselves.
- **Defenders**. Defenders must thwart malicious cyber activities on increasingly valuable and critical systems with limited resources and despite evolving technologies and threat scenarios.
- **Users**. Users — legitimate individuals and enterprises — will circumvent cybersecurity practices that they perceive as irrelevant, ineffective, inefficient or overly burdensome.
- **Technology**. As technology cross-connects the physical and cyber worlds, the risks as well as the benefits of the two worlds are interconnected.

The plan defines three research and development goals to provide the science, engineering, mathematics, and technology necessary to improve cybersecurity in light of these assumptions. The science and engineering advances needed are socio-technical in nature, and vary from foundational to applied over a range of time scales[5]:

- **Near-Term Goal** (1-3 years). Achieve S&T advances to counter adversaries' asymmetrical advantages with effective and efficient risk management.
- **Mid-Term Goal** (3-7 Years). Achieve S&T advances to reverse adversaries' asymmetrical advantages, through sustainably secure systems development and operation.
- **Long-Term Goal** (7-15 years). Achieve S&T advances for effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution.

To achieve these goals, the plan focuses on developing science and technology to support four defensive elements:

- **Deter.** The ability to efficiently discourage malicious cyber activities by measuring and increasing costs to adversaries carrying out such activities, diminishing the spoils, and increasing risks and uncertainty for potential adversaries.
- **Protect.** The ability of components, systems, users and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability and accountability.
- **Detect.** The ability to efficiently detect, and even anticipate, adversary decisions and activities, given that perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.
- **Adapt.** The ability of defenders, defenses and infrastructure to dynamically adapt to malicious cyber activities by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration and adjusting to thwart similar future activity.

[5] "Socio-technical" refers to the human and social factors in the creation and use of technology. For cybersecurity, a sociotechnical approach considers human, social, organizational, economic and technical factors and the complex interaction among them in the creation, maintenance, and operation of secure systems and infrastructure.

After a description of each element and associated research challenges, the Strategic Plan identifies research objectives to achieve in each element over the near, mid and long-term. The objectives are not comprehensive but establish a basis to measure progress in implementing the plan. These elements are applicable throughout cyberspace, although some objectives are most meaningful in particular contexts, such as cloud computing or the Internet of Things.

The plan identifies six areas critical to successful cybersecurity R&D: (1) scientific foundations; (2) enhancements in risk management; (3) human aspects; (4) transitioning successful research into pervasive use; (5) workforce development; and (6) enhancing the infrastructure for research.

The plan closes with five core recommendations:

- **Recommendation 1.** Prioritize basic and long-term research in federal cybersecurity R&D.
- **Recommendation 2.** Lower barriers and strengthen incentives for public and private organizations that would broaden participation in cybersecurity R&D.
- **Recommendation 3.** Assess barriers and identify incentives that could accelerate the transition of evidence-validated effective and efficient cybersecurity research results into adopted technologies, especially for emerging technologies and threats.
- **Recommendation 4.** Expand the diversity of expertise in the cybersecurity research community.
- **Recommendation 5.** Expand diversity in the cybersecurity workplace. Implementing the plan and these recommendations will create science and technology for cybersecurity that effectively and efficiently defends cyberspace and sustains an Internet that is inherently more secure.

2.2.2 National Privacy Research Strategy (NPRS)

The NSTC's *National Privacy Research Strategy* [NPRS] was developed in light of the US government's recognition of the challenges to personal privacy from large-scale deployment of information technology systems and from the challenges presented by Big Data.

This strategy establishes objectives and priorities for federally-funded privacy research, provides a framework for coordinating privacy research and development and encourages multidisciplinary research that recognizes the privacy needs of individuals and society and the responsibilities of the government. The overarching goal of the strategy is to produce knowledge and technology that will enable individuals, commercial entities and the government to benefit from transformative technological advancements, enhance opportunities for innovation and provide meaningful protections for personal information and individual privacy.

To achieve these goals, the National Privacy Research Strategy identifies the following priorities for privacy research in the United States:

- Foster multidisciplinary approach to privacy research and solutions;
- Understand and measure privacy desires and impacts;
- Develop system design methods that incorporate privacy desires, requirements and controls;
- Increase transparency of data collection, sharing, use and retention;
- Assure that information flows and use are consistent with privacy rules;
- Develop approaches for remediation and recovery; and
- Reduce privacy risks of analytical algorithms.

2.2.3 International Strategy for Cyberspace

The US released its first International Strategy for Cyberspace under President Barack Obama in 2011. It was the first time any presidential administration had published its vision and goals for cyberspace and cybersecurity. The strategy included several policy initiatives, which the Obama Administration described as “action lines of our strategic framework,” and included the following:

- Promoting international standards and innovative, open markets;
- Protecting US networks by enhancing security, reliability and resiliency;
- Extending collaboration with international law enforcement and extending the rule of law;

- Preparing the military for 21st century security challenges;
- Promoting effective and inclusive internet governance structures;
- Working on international development by building capacity, security and prosperity;
- Supporting fundamental Internet freedom and privacy.

The Obama Administration also outlined its cybersecurity priorities, areas in which it acted through Presidential Executive Orders and Presidential Directives. The Administration´s priorities on cybersecurity were the following:

- Protecting the nation´s critical infrastructure from cyber threats;
- Improving the nation´s ability to identify and report cyber incidents in a timely manner;
- Engaging with international partners to promote internet freedom and build support for an open interoperable, secure and reliable cyberspace;
- Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets;
- Creating a cyber-savvy workforce.

The US Congress has also acted on presidential cybersecurity priorities by passing laws, including the **Cybersecurity Information Sharing Act** (**CISA**[6]). In 2017, President Donald Trump signed **Presidential Executive Order 13800**, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The EO aims to increase the cybersecurity of federal networks, improve cybersecurity of the nation´s critical infrastructure and improve the nation´s overall cybersecurity by: engaging with international allies; ensuring the nation has strategic options to deter adversaries; and training a cybersecurity workforce.

[6] https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

3 PRIORITY AREAS FOR EU-US COLLABORATION IN R&I CYBERSECURITY AND PRIVACY

In this section, we analyze EU and US priorities in cybersecurity and privacy as well as the coverage of various cybersecurity and privacy topics in their R&I programs. We map the priorities according to the Joint Research Centre´s (JRC) taxonomy for cybersecurity and analyze resources devoted by EU and US to cybersecurity and privacy.

The JRC's taxonomy defines three vectors for categorizing 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.

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 that includes 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[7] (2016);
- Federal Cybersecurity Research and Development Strategic Plan[8] (2016);
- Secure and Trustworthy Cyberspace program[9] (SaTC), released by the National Science Foundation (NSF);
- Cyber Security Division[10] (CSD) programme of Department Homeland Security (DHS);

[7] 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.

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

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

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

- DARPA programs[11];
- IARPA programs[12].

Compared to the US, the EU's R&I activities in cybersecurity are more limited to concrete actions (versus a variety of publications and programs). We have chosen to analyze the following EU initiatives in R&I in the field of cybersecurity and privacy. These initiatives have been selected on the basis of their influence in Europe.

- Horizon 2020 R&I Funding Program[13];
- The Network and Information Security Platform initiative[14];
- Contractual PPP on cybersecurity[15] and its supporting organization European Cyber Security Organisation[16] initiative; and
- The activities of the European Union Agency for Network and Information Security[17] (ENISA).

In order to determine the overall priorities in the EU and the US, we have carried out a desktop analysis and a survey of EU-US cybersecurity stakeholders and combined the results. During the desktop analysis, the priorities highlighted in every document mentioned 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 survey analyzed in this section was carried out in 2018 and 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,

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

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

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

[14] 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

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

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

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

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 Research Domains, Technologies and Applications, and Sectors by classifying them with a value between 1 and 4, where 4 indicated the highest importance.

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 normalized 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 propagated only the value of the desktop analysis. All final tables are sorted by the total average value (for the EU and the US).

3.1 Cybersecurity Research Domains

As shown in Table 1, the overall analysis of Cybersecurity Research Domains shows that *Security Management and Governance* is the most prioritized topic, followed closely by *Data Security and Privacy* and *Education and Training*., and *Assurance, Audit and Certification*.

It is easy to note that Cryptography gets a quite low score in both the EU and the US. This can be explained by the fact that in many documents Cryptographic methods are mostly considered to be tools to progress in other topics (e.g., it is heavily used for Data Security and Privacy, which is found to be the second topic by our analysis). 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* 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 1: Total Ranking for Cybersecurity Research Domains

Cybersecurity Research Domains	AVG			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Security Management and Governance	0.89	0.79	0.84	1	0.8	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	0.82	0.78	1	0.84	0.92	0.47	0.79	0.63
Assurance, Audit, and Certification	0.76	0.79	0.78	1	0.83	0.92	0.53	0.75	0.64
Network and Distributed Systems	0.76	▨	0.76	0.73	▨	0.73	0.79	▨	0.79
Software and Hardware Security Engineering	0.7	0.78	0.74	0.62	0.78	0.7	0.79	0.77	0.78
Human Aspects	0.66	0.79	0.72	0.54	0.8	0.67	0.79	0.77	0.78
Identity and Access Management (IAM)	0.57	0.77	0.67	0.35	0.78	0.56	0.79	0.75	0.77
Security Measurements	0.58	0.74	0.66	0.73	0.75	0.74	0.42	0.73	0.58
Trust Management, Assurance, and Accountability	0.47	0.85	0.66	0.73	0.87	0.8	0.21	0.82	0.52
Operational Incident Handling and Digital Forensics	0.62	0.68	0.65	0.62	0.72	0.67	0.63	0.64	0.63
Cryptology (Cryptography and Cryptanalysis)	0.39	0.69	0.54	0.37	0.72	0.54	0.42	0.67	0.54
Legal Aspects	0.26	0.8	0.53	0.38	0.86	0.62	0.13	0.74	0.44
Theoretical Foundations	0.52	▨	0.52	0.73	▨	0.73	0.32	▨	0.32

3.2 Applications and Technologies

As shown in Table 2, *IoT* is the leader in our ranking of Applications and Technologies topics. However, for the EU, the difference between the first four positions is negligible. *Cloud and Virtualization, Mobile Devices* and *Big Data* go closely together after the leading topic. Meanwhile, *Operating System*s, ranked number five, is quite behind.

During our desktop analysis, we have noticed that US programmes are more focussed on CyberSecurity Research Domains and less on Sectors and Applications and Technologies. This explains the low scores for US, but, since we are more interested in the relative difference between the top topics, this does not cause much problems for our analysis.

Table 2: Total Ranking for Applications and Technologies Topics

Applications and Technologies	AVG			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Internet of Things	1	0.91	0.96	1	0.91	0.95	1	0.91	0.96
Cloud and Virtualization	0.71	0.86	0.79	1	0.89	0.94	0.42	0.83	0.63
Mobile Devices	0.66	0.9	0.78	1	0.89	0.94	0.31	0.91	0.61
Big Data	0.58	0.87	0.73	1	0.87	0.94	0.16	0.88	0.52
Operating Systems	0.5	0.82	0.66	0.73	0.86	0.79	0.26	0.79	0.53
Critical Infrastructures	0.63		0.63	0.63		0.63	0.63		0.63
Supply Chain	0.49	0.76	0.62	0.37	0.74	0.55	0.61	0.77	0.69
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		0.74
Hardware	0.25	0.78	0.52	0.35	0.79	0.57	0.16	0.77	0.46
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

3.3 Sectors

As shown is Table 3, *Energy* is considered the most important area in terms of sectors. It is followed by *Public Safety* and *Transportation*. Moreover, we would like to highlight the low score received by the *Transportation* sector in the US. It could be inferred that *Transportation* got a low score because it might be considered a part of *Embedded Systems* (which is an Applications and Technologies topic that scored very high score in 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 high score in the US and small score in the EU. This topic was not investigated in our survey and we cannot confirm the findings.

Table 3: Total Ranking for Sectors

Sectors	AVG			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Energy	1	0.85	0.92	1	0.86	0.93	1	0.8	0.9
Public Safety	0.83	0.89	0.86	1	0.91	0.95	0.67	0.81	0.74
Transportation	0.83	0.86	0.84	1	0.86	0.93	0.67	0.85	0.76
Financial Services	0.7	0.9	0.8	0.73	0.91	0.82	0.67	0.87	0.77
Health	0.57	0.92	0.75	0.73	0.92	0.83	0.42	0.93	0.67
Telecom	0.66		0.66	0.65		0.65	0.67		0.67
Industry 4.0	0.57		0.57	0.73		0.73	0.42		0.42
Nuclear	0.45		0.45	0.65		0.65	0.25		0.25
Water	0.45		0.45	0.65		0.65	0.25		0.25
Supply Chain	0.39		0.39	0.19		0.19	0.58		0.58

3.4 Expert analysis of our ranking

AEGIS conducted 20 in-depth interviews in Europe and the US with leading cyber security researchers and key stakeholders from the industry, in order to gather insights on the EU/US landscape on cybersecurity and privacy and on the AEGIS prioritized topics for transatlantic R&I cooperation. In short, we asked the experts whether they agree with our selection of *five top topics* for the three vectors of the analysis. Although the experts interviewed have different perspectives, in general, they share the views of AEGIS. Their insights are summarized in the following sections.

Cybersecurity Research Domains. With respect to the cybersecurity research domain, the experts have mostly agreed with our proposal. Several of them underlined the importance of economic approaches for cybersecurity management (e.g., risk management). Among the additional topics proposed by the experts we are able to single out only *Operational Security* (i.e., *Operational Incident Handling and Digital Forensics* in our taxonomy), which were mentioned by 2 participants.

Applications and Technologies. Although there were not many critics of our proposals, various experts highlighted two additional (and novel) topics that will require attention of cyber security in the nearest future: *Artificial Intelligence (Machine Learning)* and *Blockchain technologies*.

Sectors. For sector priorities, we have also got mostly positive feedbacks. *Public Safety* has received a bit controversial assessment by the participants: some of them proposed to substitute this sector with another one, while the others marked it as the most important sectors to focus on. As for missing top sectors, there was no notable agreement among experts.

3.5 Focus sectors

In addition, we would also like to highlight three sectors that have been identified as critical areas with opportunities for EU-US cooperation. The landscape of these sectors was presented to the European Commission in 2019. The following will provide a brief overview of these sectors.

3.5.1 Finance

The financial sector 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. For instance, malware installed in a user´s computer could also infect the financial institution. Overall, this causes problems for the user and the financial institution.

3.5.2 Healthcare

The Healthcare sector includes several sectors to provide goods and services to treat patients. This sector, which includes the hospital, medical and pharmaceutical industries, as well as patients, is exposed a new wide surface of cyberattacks because many elements are interconnected.

There are also possibilities of cyberattacks in the Healthcare sector 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.

3.5.3 Maritime

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

The general concern for this sector 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 sector. If the GPS System is compromised, there is potential for serious consequences.

3.6 Summary of the Analysis of the Three Focus Sectors

For the analysis of the coverage of the R&I funding needs in the three focus sectors, we specified the importance of every cybersecurity research domain and compared it with the results of our overall analysis in Table 4.

Table 4: Comparison of R&I Priorities in the US and the EU for the Three Focus Sectors

CSP Research Domains	Maritime	Health	Financial	EU priority	US priority
Assurance, Audit, and Certification	High	High	High	0.92	0.64
Cryptology (Cryptography and Cryptanalysis)	Medium	Medium	High	0.54	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 Dig. Forensics	Medium	Low	High	0.67	0.63
Human Aspects	High	Medium	High	0.67	0.78
Identity and Access Management (IAM)	High	High	High	0.56	0.77
Security Management and Governance	High	Medium	High	0.9	0.79
Network and Distributed Systems	Medium	Medium	High	0.73	0.79
Software and Hardware Security Engineering	Medium	High	Medium	0.7	0.78
Security Measurements	Medium	Medium	High	0.74	0.58
Legal Aspects	Low	Medium	Medium	0.62	0.44
Theoretical Foundations	Low	Low	Medium	0.73	0.32
Trust Management, Assurance, and Acc.	High	Medium	High	0.8	0.52

Our reasoning behind the importance of the rating is as follows. *Assurance, Audit and Certification* is high for all three sectors since the sectors are very heterogeneous (and dynamic) and rely a lot on software and hardware providers.

Cryptology is high for the Financial sector as the secrecy of transactions has to be maintained. *Data Security and Privacy* has a high importance for all sectors, since they all store, transmit and manage third party data. *Education and Training* is put to medium for Financial sector as the importance of cybersecurity in it is long recognized and much more attention has been devoted to education and training in this sector already.

Operational Incident Handling and Digital Forensics is high for the Financial sector, as it is important for tracing cyber criminals. While we have indicated low importance for the Health sector, since although prosecution of criminals in this case is required as well, it is difficult to mitigate the additional harm the attackers can do after the attack.

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

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

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

The *Software and Hardware Security Engineering* rating is a bit higher for Healthcare given that the sector has a higher reliance on IT. Because of this, attackers have more opportunities to impact people (patients) by compromising devices.

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

Legal aspects are considered of low importance for the Maritime sector, mostly because current cybersecurity measures for this sector are not well developed and this issue yet to come into play for the sector.

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

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

In our analysis, we found out that in the majority of cases, the most important cybersecurity research domains are well covered by existing R&I programs. There are only a few topics, which are described below, that require specific attention.

First, we would like to underline the striking difference between the moderately high demand for *Cryptography* in many sectors and lack of attention paid to this area by R&I programs in both the EU and the US. A possible explanation for this mismatch could be the fact that cryptography is often seen as means to achieve other goals, e.g., it is heavily used for *Data Security and Privacy* (which has high score in our ranking). 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 high 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 sectors require strong evidence of compliance with various standards and legislations. A similar situation can be observed with the *Trust Management, Assurance and Accountability* topic.

We see only moderate attention in EU to such hot topic as *Identity and Access Management.* The EU could explore this research domain 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 moderately important for many Applications and Technologies 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, technical support and vision is required for the correct formulation and enforcement of cybersecurity laws.

Overall, there is still a lot of work to be done in cybersecurity R&I on both sides of the Atlantic to increase resilience and response. Nonetheless, identifying common priorities is helpful when deciding what issues to tackle first and where to invest to R&I funding. It is also useful to consider what areas are not considered priorities and perhaps consider whether that assessment is still valid today.

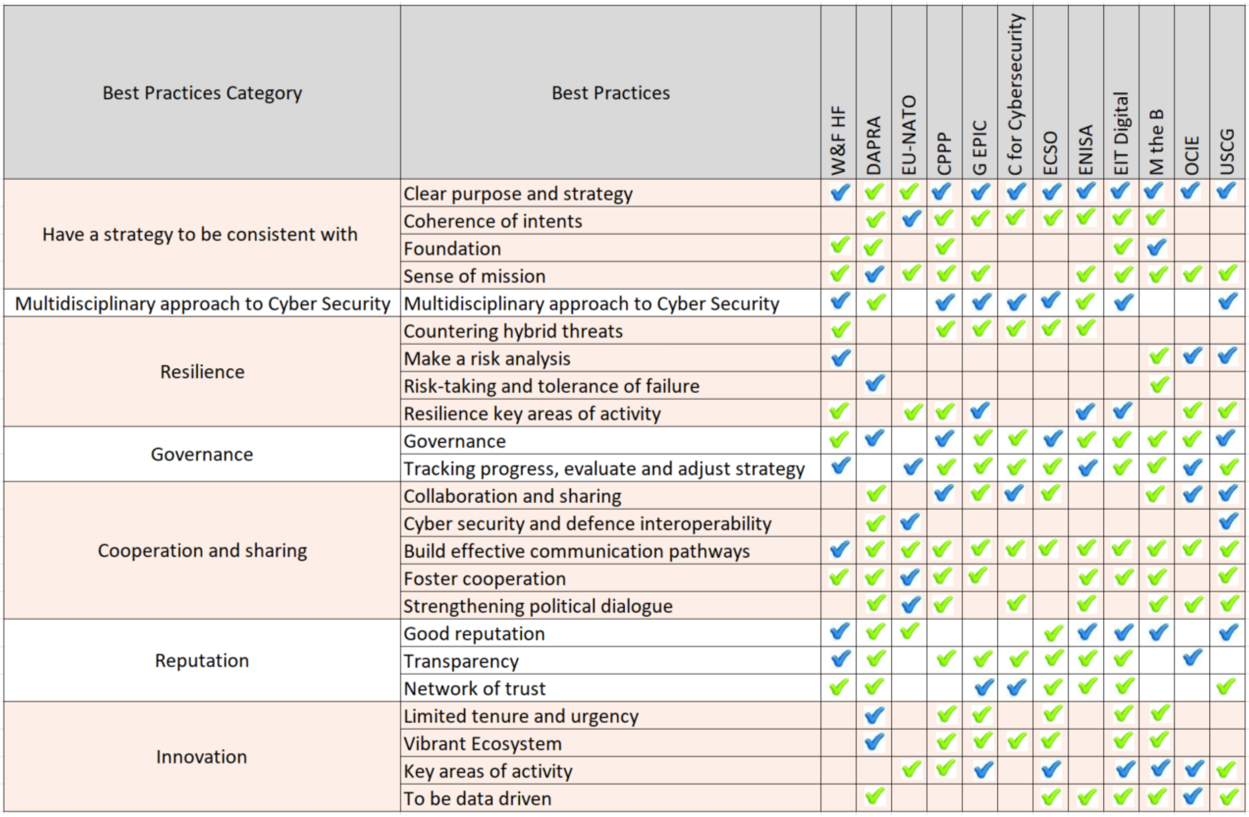
4 INNOVATION PARTNERSHIPS IN CYBERSECURITY AND PRIVACY

Security challenges require international collaboration on an unprecedented scale, including the promotion of strong cybersecurity measures to protect government and the world economy. Communication around cyber and physical security is extremely important to success. Polices need to be explained and everyone should understand how their behavior can make a difference.

To achieve this, we must focus on fostering collaboration between organizations from EU and US. These innovation partnerships increase privacy and trust and protect collective interests by sharing leading best practices and proven cybersecurity solutions.

Common approaches that represent good practices in order to enable mutually beneficial partnerships between different organization from EU and US are presented in the following table.

Table 5: Best Practices to Foster Cybersecurity Collaboration Between EU-US Entities



Best Practices Category	Best Practices	W&F HF	DAPRA	EU-NATO	CPPP	G EPIC	C for Cybersecurity	ECSO	ENISA	EIT Digital	M the B	OCIE	USCG
Have a strategy to be consistent with	Clear purpose and strategy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Coherence of intents		✓	✓	✓	✓	✓	✓	✓	✓	✓		
	Foundation	✓	✓		✓					✓	✓		
	Sense of mission	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
Multidisciplinary approach to Cyber Security	Multidisciplinary approach to Cyber Security	✓	✓		✓	✓	✓	✓	✓	✓			✓
Resilience	Countering hybrid threats	✓			✓	✓	✓	✓	✓				
	Make a risk analysis	✓									✓	✓	✓
	Risk-taking and tolerance of failure		✓								✓		
	Resilience key areas of activity	✓		✓	✓	✓			✓	✓		✓	✓
Governance	Governance	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Tracking progress, evaluate and adjust strategy	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cooperation and sharing	Collaboration and sharing		✓		✓	✓	✓	✓			✓	✓	✓
	Cyber security and defence interoperability		✓	✓									✓
	Build effective communication pathways	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Foster cooperation	✓	✓	✓	✓	✓			✓	✓	✓		✓
	Strengthening political dialogue		✓	✓	✓		✓		✓		✓	✓	✓
Reputation	Good reputation	✓	✓	✓				✓	✓	✓	✓		✓
	Transparency	✓	✓		✓	✓	✓	✓	✓	✓		✓	
	Network of trust	✓	✓			✓	✓	✓	✓	✓			✓
Innovation	Limited tenure and urgency		✓		✓	✓		✓		✓	✓		
	Vibrant Ecosystem		✓		✓	✓	✓	✓		✓	✓		
	Key areas of activity			✓	✓	✓		✓		✓	✓	✓	✓
	To be data driven		✓					✓	✓	✓	✓	✓	✓

(✓) the best practice - case study association found during desk research phase

(✓) the ones identified with added methodology steps

4.1 Clear purpose and strategy

In order for partnerships to work, stakeholders must outline their goals and the initiatives that will be taken to achieve them. For instance, the Public-private collaboration strategy is a contractual collaboration between the public sector and a private entity in pursuit of a common objective.

A successful implementation needs to include expertise, policy guidelines and regulations and careful scrutiny and precaution before involving the stakeholders in the process.

In many cases, circling a strategic document among stakeholders along with a list of activities and an implementation plan helps characterize characterize the scope of work. It also helps make the interests accessible and clear to those involved. Finally, having a precise strategy and properly implementing it assures that the goals will be achieved.

4.2 Multidisciplinary approach

Cybersecurity is a fundamentally multidisciplinary topic and involves all sectors of people's lives, not only computer science but also political science, management, mathematics, engineering and economics. Securing the world's information and communications systems requires combining expertise from numerous fields, including engineering and technology, management, social science and policy.

Organizations from different areas present issues related to the security of data and the protection against malicious attacks.

A multidisciplinary data security approach, integrating technological with legal and communication considerations, anticipate future problems and can help businesses manage the heightened scrutiny of their data security practices.

4.3 Resilience

Resilience is defined as "*the capacity to recover quickly from difficulties*" and is an enabler for cooperation and partnerships. For an organization, it's important to be able to identify, assess and manage the risks associated with network and information systems. Further steps for monitoring and controlling the network and information systems can help detect potential cybersecurity incidents before they can cause any significant damage.

Traditionally, many enterprises have focused too heavily on protecting against cyberattacks, but a resilience-based approach is now vital to better adapt to change.

4.4 Governance

Cybersecurity is a rapidly growing field that affects governments, organizations and individuals. Every organization needs to have a complete cybersecurity framework to fully address all of its cybersecurity needs. Providing details about an organization's activities and practical information about processes and procedures will facilitate collaboration. For this reason, governance can be considered an enabler for the industry for engagement in cybersecurity and privacy R&I projects.

4.5 Cooperation and sharing

The need for information sharing is a factor that highlights the importance of trust and mutual assurance between the public and private sectors. Moreover, a clear understanding of cybersecurity and information about how private and public institutions can position themselves within a secure network of information. Information sharing is an overall best practice in dealing with cyber-threats.

4.6 Reputation

A good reputation leads to an improved network of relationships. The more people you know, the more opportunities you will have. Having a good reputation is crucial to getting people to pursue, trust and engage with your business. The trust and confidence of the communities can have a direct and profound effect on an initiative's success. Recently, the importance of reputation has become increasingly apparent in cybersecurity partnerships.

4.7 Innovation

Innovation is essential for the growth of any company and organization. The secret of success of innovative organizations is associated with their ability to get the best out of the creative tanks of their employees. Innovation can also help develop original concepts while giving the innovator a proactive, confident attitude to take risks and get things done.

5 CYBERSECURITY POLICIES ENABLING EU-US COLLABORATION

In recent years, policymakers in the EU and the US have tackled various policy areas related to cybersecurity and privacy. The areas that have seen the largest amount of activity over the past few years include: standards and certification; privacy and data protection; and public-private information sharing. In some areas, legislators on both sides of the Atlantic have taken similar approaches to regulating cybersecurity and privacy. However, in others, they couldn´t be further apart.

Understanding the basis for each region´s policies is critical to collaboration and can lead to the creation of mutually beneficial transatlantic cybersecurity policy. The following section will provide a brief overview of the major legislative actions policymakers have either adopted or are actively working on in cybersecurity and privacy. Some laws cover more than one policy area. For instance, a law that regulates standards and certification could also include provisions on public-private information sharing. Given that this section is about understanding the current policy landscape, priority will be given to legislation that has already entered into force.

5.1 Standards and Certification

Cybersecurity standards and certification is an area that has been scrutinized by lawmakers in the EU and the US for years. Although each region has acknowledged the importance of standards and certification for individual residents, the industry and the public sector, stakeholders have taken a different approach to policymaking, and as such, has achieved different results. The biggest difference in policymaking comes down to one thing: regulation. The EU has decided to strictly regulate this policy area, while the US has opted for creating voluntary standards.

EU Policies

EU lawmakers have prioritized the cybersecurity of Member State systems, Operators of Essential Services, electronic identification and ICT security products. This has led to regulation, or proposed regulation, of all of these areas. These actions are in line with the EU´s cybersecurity strategy, which is a priority for the bloc.

NIS Directive

The Directive on Security of Network and Information Systems (NIS Directive) was implemented in the EU in 2018. The directive aims to increase the overall level of cybersecurity in the EU by requiring Member States to be adequately prepared to respond during and after a cybersecurity breach. Under the NIS Directive, EU Member States must establish a Computer Security Incident Response Team (CSIRT), a national NIS authority and a national NIS strategy.

The NIS Directive also affects so-called Operators of Essential Services, or companies in certain sectors that are vital for the European economy and society and rely on ICT. These companies must adopt what the EU classifies as state of the art security approaches that are appropriate to manage the risks posed to their systems.

eIDAS Regulation

Another aspect of standards and certification the EU has been working on is the eIDAS Regulation, a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. eIDAS requires all EU Member States to mutually recognize the national electronic identification schemes used by the bloc´s members. eIDAS aims to allow citizens to use their national eIDAs to securely access online services – such as those provided by public administrations or certain private service providers – provided in other EU countries. Notably, eIDAS establishes three different types of electronic signatures: simple, advanced and qualified. Each type of signature has a different level of privacy and security.

Cybersecurity Act

Over the past few years, the EU has been analyzing whether to unify cybersecurity standards for ICT security products for all Member States. To address this, it enacted the Cybersecurity Act in 2019. Besides giving the EU Agency for Network and Information Security (ENISA) a permanent mandate, the regulation transforms ENISA into a stronger EU Cybersecurity Agency in charge of capacity building, operational cooperation, international cooperation and cybersecurity certification, among other tasks.

In addition, the Cybersecurity Act creates a framework for European Cybersecurity Certificates for products, processes and services in the EU. The framework ensures a common cybersecurity certification approach in the internal European market and improves the overall security of digital products in the Union.

US Policies

While EU lawmakers have decided that regulation is the best way to ensure that Member States and private companies adopt high cybersecurity standards, US lawmakers felt that the best approach was to create a flexible framework, called the NIST Framework, that could be adopted on a voluntary basis by the private industry. The framework is the most significant set of standards adopted by the US thus far, although it has also adopted laws related to the use of electronic signatures. Nonetheless, in light of GDPR and high profile data breaches, legislators are currently working on regulations in this area.

NIST Framework

In 2014, the National Institute of Standards and Technology (NIST) released its Cybersecurity Framework, often referred to as the NIST Framework. The framework is a voluntary set of standards and industry best practices that help an organization identify, prioritize, manage and/or communicate cyber risks. It is not meant to be a one-size-fits-all approach, as what is appropriate for one organization could be ineffective for another. Rather, the framework was designed to be technology- and industryneutral, meaning that it can be used by a wide range of organizations in different sectors. It can also be adapted to an organization´s specific needs, which may differ based on industry, size and cybersecurity risk. The framework is a living document, meaning that it can be improved as “technologies and threats evolve.”

Uniform Electronic Transactions Act

The Uniform Electronic Transactions Act (UETA) was adopted in 1999 and provides individual states in the US with a framework to authorize electronic signatures in commercial and government transactions. UETA is not a federal law, and therefore had to be adopted on a state-by-state basis. The act was limited because it only authorized electronic signatures within states. Therefore, customers that wanted to use electronic signatures for business in different states could only do so if that state had also adopted the UETA framework. This gap in access inspired legislators to develop an all-encompassing law on a federal level.

Electronic Signatures in Global and National Commerce Act

The Electronic Signatures in Global and National Commerce Act (the E-Sign Act) is a 2000 federal law that allows for the use of electronic signatures on official documents as long as the person has consented to such use and has not retracted their consent. The law authorizes the use of electronic signatures across individual state lines within the US.

CISA Act of 2018

In 2018, the US Congress approved the Cybersecurity and Infrastructure Security Act (CISA Act). The act created the Cybersecurity and Infrastructure Security Agency (CISA) and tasked it with protecting US critical infrastructure from physical and cyber threats. CISA coordinates and collaborates with other federal government agencies, private organizations and international partners to carry out its mission.

5.2 Privacy and Data Protection

Privacy and data protection is another area that both regions agree must be regulated. Unsurprisingly, they differ in the how. The EU has decided to regulate this area horizontally with two far-reaching directives: the General Data Protection Regulation and the NIS Directive. The US has taken a drastically different approach, choosing instead to regulate privacy and data protection by sector and type of information, which has resulted in a litany of laws. Although there are ongoing conversations about a national data protection law in the US, lawmakers have not reached a consensus on what such legislation should entail.

EU Policies

In this area, the EU has implemented the General Data Protection Regulation (GDPR), which is considered the world´s strictest privacy and data protection law. The law not only imposes strict rules on third countries doing business in the EU, it also requires EU-based companies and entities to comply with GDPR standards, prioritizing the protection and privacy of the region´s residents above all.

GDPR

The GDPR, which was implemented in May 2018, is the most significant piece of EU legislation that has been passed in the privacy and data protection policy space. It aims to protect all data subjects who are in Europe from privacy and data breaches and harmonize data protection laws in the EU. The law regulates how businesses and entities obtain user data, how they process it and how they protect it. It includes existing EU privacy regulations such as the Right to be Forgotten and provisions regarding international data transfers.

Nonetheless, GDPR also includes new concepts, such as increased territorial scope, which means that the law applies to businesses established in the EU and those established outside the bloc. It also includes concepts such as data portability, which requires organizations to give individuals their personal data in a standard, machine- readable format when requested. Notably, GDPR takes violations of the law seriously. Enforcement authorities can fine businesses up to 4% of their worldwide turnover or €20 million, whichever is greater.

US Policies

Unlike in the EU, the US has no comprehensive federal data protection law, although lawmakers have been coming under increasing pressure to develop one. The closest equivalent is the Privacy Act of 1974. Instead, the US relies on what some have described as a "patchwork" of federal laws, state laws and regulations, many of which are sector-specific. As a result, some of these laws apply to categories of information, such as financial or health information, while others apply to activities that rely on personal information for their execution, including telemarketing and marketing via email. In addition, these laws sometimes overlap and contradict one another. We will not cover all of the US laws related to data protection and privacy due to the sheer amount of them that exist.

In addition, the US system contains guidelines and frameworks, which are self-regulatory and voluntary standards that are not enforceable by law. Also relevant are consumer protection laws that are not privacy laws per se, but that also have aspects that dictate the protection and disclosure of personal data.

Privacy Act of 1974

One of the most important hallmarks of US privacy policy, and by extension cybersecurity policy, is the Privacy Act of 1974. In essence, the law "regulates the collection, maintenance, use and dissemination of personal information by federal executive branch agencies." It provides individuals with the right to request the records a federal agency has on them; the right to request a change to their records in the spirit of accuracy, relevance and completeness; and the right to be protected against an unwanted invasion of privacy due to the "collection, maintenance, use and disclosure of their personal information." The law requires agencies to publish their system of records in the publicly accessible Federal Register.

EU-US Policies

Interestingly, data protection and privacy is one of the few areas in cybersecurity where the EU and US have an official agreement in place, which is called Privacy Shield. This is perhaps due to the type of activity the agreement covers: the transfer of information across the Atlantic.

Privacy Shield

Privacy Shield is an agreement that regulates the transfer of European users´ data to the US for commercial purposes and prevents the US government from having unlimited access to European data. It also provides EU residents access to "accessible and affordable" dispute resolution mechanisms.

The bilateral agreement went into effect in 2016 and is referred to as the Privacy Shield Framework. It requires companies that transfer European users´ data outside the EU to self-certify to the US Department of Commerce that they meet the framework´s requirements and publicly commits to continue doing so. More than 3.300 organizations use Privacy Shield for their transatlantic data transfers, including Facebook, Google, Microsoft, Amazon and Twitter.

The European Commission and the US Department of Commerce carry out an annual joint review of Privacy Shield.

5.3 Public-Private Information Sharing

Public-private information sharing is a policy area in which both the EU and the US have adopted regulations to promote the sharing of data between states as well as between the public and private sectors. In this area, the regions have adopted similar approaches, although one difference remains: the force of law. As with other policies, the EU has mandated public-private information sharing, while the US has strongly encouraged it and has put in place mechanisms to foment the exchange.

EU Policies

The concept of public-private information sharing is enshrined into EU law. However, unlike the US, which has created specific laws to encourage information-sharing, the EU includes this concept in its hallmark data protection and privacy laws: GDPR and the NIS Directive.

GDPR

The GDPR established public-private information sharing for data controllers and data processors. Notably, the law makes information sharing mandatory during and after data breaches and in situations where it is necessary in order to comply with legal obligations. Under GDPR, a data controller must notify data protection authorities of a breach within 72 hours of becoming aware of the incident and inform the subjects whose data has been compromised "without undue delay."

The law also requires data processors – third-party companies that process data for their customers, known as data controllers – to notify data controllers without undue delay of a security breach after they become aware of such an incident. In this situation, the data controller has the legal responsibility of notifying the relevant data protection authorities.

NIS Directive

Like GDPR, the NIS Directive requires Operators of Essential Services to report cybersecurity breaches that meet certain criteria to the appropriate data protection authorities. In contrast to GDPR, the NIS Directive provides some liability protection for the entity reporting the breach, stating that "notification shall not make the notifying party subject to increased liability." This characteristic is also present in US public-private information sharing legislation.

US Policies

As noted above, the US has also been active in the area of public-private information sharing. Nonetheless, it has decided that the practice is of such importance that it deserves its own law. Like other aspects of US cybersecurity policy, the laws that govern public-private information sharing are meant to foment the practice, not make it mandatory.

Cybersecurity Information Sharing Act (CISA)

In order to promote public-private information sharing between private organizations and the federal government, among others, the US Congress passed the Cybersecurity Information Sharing Act (CISA) in 2015. CISA allows companies to monitor cybersecurity threats and implement defensive measures on their systems in response. It also provides safeguards in order to promote information sharing between private companies and local, state and federal governments as well as between private companies.

Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

The CLOUD Act was approved by the US Congress in 2018. It was created to streamline how US and international law enforcement agencies obtain digital personal information stored by US tech companies in different territories. The law requires US technology companies to provide requested data to US law enforcement agencies even if such information is stored in another country.

It also allows the US to enter into bilateral access agreements with other countries in order to ensure international authorities have similar access to information stored in each country.

The main policy differences between the EU and the US are summarized in the table below.

Table 6: Comparative Analysis Between EU and US Cybersecurity Policies

Policy Area	Similarities	Differences
Standards and certification EU policies analyzed: NIS Directive, Cybersecurity Act, eIDAS US policies analyzed: NIST Framework, Electronic	**Improve cyber preparedness**. The NIS Directive and the NIST Framework aim to improve cyber preparedness across the board.	**Law vs. voluntary standards**. The NIS Directive is a law that must be followed by all EU Member States and Operators of Essential Services. NIST is a voluntary framework that

Policy Area	Similarities	Differences
Signatures in Global and National Commerce Act, Uniform Electronic Transactions Act, CISA Act of 2018	**Use the best cybersecurity measures available**. The NIS Directive and the NIST Framework call on entities to use the best available measures to protect their systems. **Dedicated agency for cybersecurity focused on protecting critical infrastructures**. The Cybersecurity Act established the ENISA as the region´s cybersecurity agency. The US equivalent is CISA.	organizations can choose to adopt if they so wish. **Cybersecurity certification framework**. The EU has established voluntary governmental certification schemes for ICT products and services. The US does not provide federal certification for such products and relies on voluntary industry certification. **Electronic ID certification and trust services**. The EU´s eIDAS regulates electronic identification and trust services, e.g. electronic signature, electronic seals. The US also regulates electronic signatures but has not taken action on trust services.
Privacy and data protection EU policies analyzed: GDPR, Privacy Shield US policies analyzed: Privacy Shield, various laws affecting commerce, children´s online privacy, financial services, health, credit reporting and electronic communications	**Certain information must be protected**. The GDPR and the various US laws concerning privacy clearly establish that there are some types of information that must be protected at all costs. Information on EU residents transferred to the US must be protected. Privacy Shield established clear safeguards for how to handle EU resident data. **Spam protection**. The EU and the US recognize that spam is a problem and attempt to cut down on the amount of spam users receive with specific proposed regulations and current implemented regulations.	One regulation vs. various regulations. With the GDPR, the EU has established the same rules for all sectors that collect data. The US has taken a different approach, regulating specific sectors. **Streamlined enforcement**. The GDPR establishes data protection authorities to ensure compliance. Enforcement is not as streamlines in the US, where different agencies regulate different sectors. **Liability protection**. CISA recognizes that one of the barriers to information sharing is liability, and thus provides liability protection. The NIS Directive also provides this, although GDPR does not.
Public-Private information sharing	**Recognized need for information sharing**. With the	

Policy Area	Similarities	Differences
EU policies analyzed: NIS Directive, GDPR US policies analyzed: CISA Act of 2015	GDPR and the NIS Directive, the EU established the importance of sharing information. In the US, CISA established communication channels for the public and private sectors.	

Although it might be instinctive to compare EU and US cyber actions side by side, as we can see, it is not always possible. Nonetheless, it is important to try to understand each region´s approach to regulation as well as accept that there may be some areas or issues that the jurisdiction in question does not want to legislate.

This exercise allows policymakers to collaborate with their foreign counterparts more effectively and develop policies or frameworks that are mutually beneficial to both the EU and the US. It is clear that creating identical legal landscapes will be impossible, especially considering the different ideologies on both sides of the Atlantic, but it may be possible to develop a shared common ground. If two of the world´s largest economies and cyber players can reach a consensus, it will no doubt shape policy in important ways for years to come.

6 RECOMMENDATIONS FOR EU-US COLLABORATION IN COLLABORATION

There is no doubt that the theme of cybersecurity, both in its broadest sense as well as in the multiple sectors with which it intersects, is of paramount importance for transatlantic dialogue and collaboration. Recent years have seen many pivotal changes in cybersecurity and privacy policy in both the EU and US.

Political and economic realities as well as different stages in development of private sector maturity in cyber space have significant impact on the types of policies a particular nation pursues and its corresponding receptivity to collaboration. Below are listed recommendations that offer promise for transatlantic cybersecurity collaboration.

- **Awareness about the benefits of cybersecurity cooperation**: Raise awareness among thought leaders, policy makers and elected officials enlisting their role as champions and unofficial ambassadors about the myriad advantages of pursuing deeper connections and cooperation in the cybersecurity sector. Such awareness can be created through low-cost means including real-time information and insights delivered through the web and various social media campaigns to promote the benefits of cooperation.
- **Adopt a common and harmonized language for stakeholder communication to accelerate EU-US collaboration**. This goal can be achieved through requests for feedback in consultation with relevant industry representatives to advise and inform government officials who are charged with developing agreed-upon terms and taxonomy. This approach also advances improved communication, training and interactions among policy makers and industry in cybersecurity and privacy.
- **Create idea exchanges between the public and private sectors**. Explore and develop structures and means to inform private sector enterprises about best practices in scaling innovative technology and monetizing acceptable risk through attracting venture capital to do so. Research focused public-private operational models have already been implemented, as

demonstrated by globally well-regarded organizations such as DARPA (Defense Advanced Research Projects Agency) and MITRE Corp. for strategic inspiration to meet cyber challenges through break-through technology. Implementation of such idea exchanges could include tie-ups between similar industry associations for cross-mentoring of EU and US member companies, online delivery of tutorials and organization of virtual workshops with VC funders and successful entrepreneurs.

- **Establish a new mechanism for more effective coordination among cybersecurity agencies and stakeholders on both sides of the Atlantic**. Different regulatory postures regarding the global cybersecurity environment can lead to legal conflicts between countries and have a chilling effect on R&I collaboration as well as private sector investment. As a potential remedy, a web-based "clearing house" mechanism could be created to eliminate legal compliance conflicts for EU and US entities. Such coordination requires expanded collaboration among key players like the European Commission, ENISA and Member States on the EU side. In the US, coordination would include the agencies working on cybersecurity policies through the interagency process and establishing closer official and informal relationships with European decision-makers to accelerate achievement of mutual objectives.
- **Promote the adoption of a unified approach based on international standards to foster collaboration in cybersecurity R&I across the Atlantic**. Government agencies, the private sector, academia and research communities should collaborate on developing common standards through leveraging of existing avenues of communication. Because industry reacts quickly to the needs and desires of its customers, the feedback from companies engaged in these sectors will be invaluable in achieving competitive advantages of benefit to both transatlantic enterprises and policy makers. Collaboration on the development of common standards in ICT would ensure standards remain voluntary, consensus-based and market-led. A unified approach will allow EU researchers to develop products and services that have the capabilities to compete in the highly-competitive US market and other international markets.

- **Create a platform such as through the NIS Cooperation Group that would help enhance the sharing of information on threats and best practices at an international level**. This would require better coordination among key players like the EC, ENISA and Member States on the EU side, and the US agencies involved in cybersecurity policies through the interagency process including the US Department of Commerce, NIST, the Department of Homeland Security and the intelligence community. By doing so, synergy and collaboration among the agencies in charge of the NIST Framework and those in charge of the implementation of the NIS Directive and the GDPR will accelerate and result in a common framework, taxonomy and risk-based language, standards and practices that would facilitate cybersecurity compliance for companies in the EU and the US.
- **Join forces in the battle against fake news**. “Fake news” and other methods of cyber disinformation have become a scourge on all elements of global society and preventing its dissemination could be a well-regarded goal for transatlantic policymakers. Preventing such news from appearing and spreading, especially in social media, requires new models for social network influence, language processing, fake account detection, and identifying and addressing deep fakes, among other tactics.

7 CONCLUSIONS

The realm of cybersecurity and all that it encompasses is revolutionizing the technology landscape between Europe and the US. Thus, it is of paramount importance that the transatlantic partnerships navigate the challenges ahead so that the vibrancy, health and mutual benefits of the relationship are sustained.

Relevant policies that influence future research and innovation collaboration between the EU and the US in the field of cybersecurity and privacy have been addressed in this chapter and include standards and certification; privacy and data protection; and public-private information sharing.

Regarding standards, the EU and the US do not have shared or mirrored pieces of legislation. In the US, the focal point for standards is the NIST Framework, issued in 2014 to improve critical infrastructure cybersecurity and built on voluntary consensus standards and industry best practices. At the EU level, the NIS Directive went into effect in 2018. Additionally, the European Commission's Cybersecurity Act, which creates an EU certification framework for ICT security products, aims at unifying cybersecurity standards for all Member States. While the NIS Directive applies not only to EU Member States, but also US companies doing business in the EU, the NIS Framework is not obligatory for any entity.

In the privacy and data protection area, the US and the EU have adopted different strategies towards regulation. The EU follows a cross-cutting policy approach through GDPR and the new e-Privacy Regulation, while in the US there is no comprehensive federal data protection law. Instead, the US has opted for an approach tailored to specific sectors and types of information, including among many others, the financial and health information sectors.

Regarding public-private information sharing, there is a transatlantic consensus about the role that information sharing plays to prevent and mitigate cybersecurity attacks that also affect private companies, in particular, Operators of Essential Services and Digital Service Providers. From this perspective, certain mechanisms for sharing information have been implemented through legislation and policies on both sides of the Atlantic. On the EU side, this has been done through the GDPR and NIS Directive, while the US has adopted CISA and the CLOUD Act. In fact, sharing information across borders is an opportunity to reinforce transatlantic collaboration, since cross-border cyber incidents will continue to occur.

The analysis of these policies and legislation demonstrates the complexity of the issues surrounding cybersecurity and privacy and the multiple players involved in monitoring problems and implementing solutions, especially in the US. Unlike in the EU, where specific agencies work on the European Commission´s cybersecurity priorities and strategies, the US sets and enforces its national security policies, including cybersecurity policy, through the National Security Council Interagency Process, where multiple players are involved.

Nevertheless, the comparative analysis of EU and US policies on cybersecurity and privacy demonstrates that notwithstanding the differences, many transatlantic approaches to cybersecurity are aligned that can provide common ground for cyberspace harmonization and cooperation between the US and the EU.

In sum, strengthening EU-US dialogues and improving cooperation on cybersecurity and privacy research and innovation is not about eliminating policy differences. Rather, the goal is to develop a set of measures that acknowledge these differences and establish a common ground for collaboration that maximizes commonalities and synergies between EU and US policies and legislation on cybersecurity and privacy.

REFERENCES

[Fed_Strat_Plan] Federal Cybersecurity Research and Development Strategic Plan, https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf (February, 2016)

[Enh_Act] Executive Order (EO) 13636 - Improving Critical Infrastructure Cybersecurity https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[Cyber_Strat] Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, available at

https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf (2011).

[NPRS] National Privacy Research Strategy, (June, 2016) https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf

[BIG_DATA] Executive Office of the President, Big Data, seizing Opportunities, Preserving Values https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May, 2015).

[PCAST] Executive Office of the President, President's Council of Advisors on Science and Technology (PCAST), Big Data: A Technological Perspective, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[Int_Strat] Executive Office of the President, International Strategy for Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. (2011)

[EO_13800] Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (2017).