ACTIONS FOR EU-US CYBER DIALOGUE

Authors: Claudio Caimi (HPE), Dan Caprio (The Providence Group), Jim Clarke (WIT), Jonathan Litchman (The Providence Group), Fabio Martinelli (CNR), Camille Sailer (EACCNJ), Jody Serrano (Inmark), Alberto Terzi (HPE), Yolanda Ursa (Inmark), Rebecca Wright (Rutgers), Artsiom Yautsiukhin (CNR)

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

1 INTRODUCTION

The AEGIS project, a Horizon 2020 initiative that aims to foment EU-US cooperation on cybersecurity and privacy research and innovation (R&I), understands cybersecurity´s critical role; AEGIS has worked to identify priority areas to accelerate cybersecurity and privacy cooperation between the EU and the US. Although both jurisdictions must improve cybersecurity resilience across all sectors, **AEGIS has selected three sectors that belong to critical infrastructures for cybersecurity and stand out for mutually beneficial transatlantic cooperation: finance, healthcare and maritime sectors**.

These sectors have been identified as critical from the point of view of cybersecurity needs both in the EU and US cybersecurity strategies and policies. The EU classified **finance** as a critical sector in the Network and Information Security Directive (NIS Directive).[1] The US also defined finance as a critical infrastructure sector in 2013 and tasked the National Institute of Standards and Technology (NIST) with developing a framework to assist critical infrastructure operators.[2] More recently, in 2018, the Trump Administration stated that it would prioritize risks across seven key areas, including banking and finance, in its National Cyber Strategy.[3]

The **health sector** has also been identified as a priority by EU and US policymakers. Health is one of the critical sectors in the NIS Directive. Additionally, the sector is one of few examples of proven EU-US collaboration in R&I, as both regions actively cooperate to fund researchers from both regions through Horizon 2020 and equivalent US programs.[4] The US, meanwhile, considers health a critical infrastructure sector. The health sector in the US also benefits from the NIST Framework. In 2018, the Trump Administration maintained health as one of its seven critical infrastructure priority areas in its National Cyber Strategy.

Finally, the **maritime sector** is also considered critical. The EU has classified maritime cybersecurity a priority since the early 2000s, when it passed the 725/2004 Law on Enhancing Ship and Port Facility Security.[5] The maritime sector is also considered a critical sector under the NIS Directive. The US also prioritizes maritime cybersecurity and defines it as a critical infrastructure sector. The Trump Administration has placed special attention on maritime cybersecurity in its National Cyber Strategy. The country has pledged to act quickly to strengthen maritime cybersecurity in the country with a number of key initiatives.

This document is part of the AEGIS´ contribution to the EU-US dialogues on cybersecurity. It briefly outlines potential topics for EU-US collaboration in these areas as well as the challenges faced. The document also provides actions to enhance collaboration in these sectors in the short term. In addition, the document provides an overview of three cybersecurity policy areas – standards and certification, data protection and privacy and public-private partnerships – that impact bilateral cybersecurity dialogues and R&I and proposes a series of actions to stimulate EU-US cooperation in cybersecurity policy.

[1] European Union Agency for Network and Information Security. *NIS Directive* https://www.enisa.europa.eu/topics/nis-directive

[2] Obama Administration (2013). *Presidential Policy Directive – Critical Infrastructure Security and Resilience* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[3] Trump Administration (2018). *National Cyber Strategy of the United States of America* https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[4] EC. *EU-US in Horizon 2020. Societal Challenge 1: Health, demographic change and well-being* https://ec.europa.eu/research/health/pdf/factsheets/factsheet_eu-us.pdf

[5] *Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on Enhancing Ship and Port Facility Security* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:en:PDF

2 RESEARCH ACTION AREAS

AEGIS proposes to focus on those cybersecurity topics that require a cross-organisational and international approach to addressing cybersecurity and privacy, which will encourage researchers to consider multi-stakeholder domains and face the issues caused by different regulations and administrations.

2.1 Finance

The financial sector is one of the most targeted by cyber criminals, mostly because of the direct way of getting financial benefit out of its abuse (stealing market plans, know-how, compromising private identifiable information, stealing credit cards and executing fraudulent transactions, cryptocurrency market, etc.). When it comes to products such as online banking and other financial services, the user is alone and must protect him/herself. This could cause consequences in other areas of the financial sector. For example, malware installed in a user´s device, could penetrate the financial service´s network. Prosecution of criminals is a difficult task for the law enforcement units as the attackers often hide behind international borders.

2.1.1 Topics for EU-US collaboration

The following topics were selected for the finance sector:

- *Fighting fake news.* News has great influence on the stock market. Consequently, so does fake news, which is deliberately spread by fraudsters in order to gain advantage from unexpected changes (and even panic) on the stock market. Preventing such news from appearing and spreading (especially, in social media) requires new models for social network influence, language processing, fake account detection, identifying and addressing deepfakes, etc.
- *Cybersecurity assurance, certification and responsibility.* Need to agree on common standards and certifications that facilitate data flow and trusted security among end-users along the whole supply chain. For example, the possibility to move a part of a business to the Cloud facilitates many business activities, which bring a number of cybersecurity questions: "how to select the most secure provider?", "how to be sure that the provider maintains its promises?" Furthermore, the crisis/incident management in such environment and sharing the responsibility for its mitigation is a problematic issue as well, in the international context, as many cloud providers are located in other countries comparing to their users.
- *Cyber Insurance*. Cyber insurance is a relatively novel way of distributing cyber security exposure, which gains popularity in the most cyber security advanced organisations. Moreover, by enforcing regulatory measures (e.g., targeting taxes, obligatory certification, increased liability, etc.) a government may influence the cyber insurance market to increase the welfare of the society in general (e.g., fast virus propagation prevention due to high security and fast reaction of key network elements). As Europe is lagging behind US in both overall premium and number of insurance providers, collaboration in this field could help EU to raise its skills in the subject and foster a new promising market.
- *Data security and privacy*. Financial organisations collect huge amount of data by conducting their business (e.g., transactional data) as well as by collecting the information for their business (e.g., information about a potential insured). The privacy of users must be protected while the data are stored, processed and disposed.
- *Security of new distributed business models*. Distributed Ledger Technologies (DLT), such as Blockchain, need more dedicated risk evaluation, as for cryptocurrencies. For example, one issue to be dealt with is cryptography, which is essential for DLTs and could be challenged by the quantum technologies.

2.1.2 Challenges

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

2.1.3 Actions

Action	What to do	How to do it
A1	**Agree and prioritize on finance certifications, standards and cyber security regulations** to be harmonized and how.	Create finance cybersecurity **collaboration frameworks** on able to operate under different jurisdictions without violation. Focus on projects that help to reduce the differences in legislations, standards and certification schemes, especially, regarding young technologies as **IoT, cloud and virtualization, DLT**, etc.
A2	Support R&I projects aiming for complex and distributing **crisis management actions**.	**Engage key actors** (e.g., law enforcement agencies, providers along the supply chain, ISPs, etc.), and consider the whole process including defining requirements and responsibilities, quick and coordinated reaction, and collaborative recovery. Commit funding agencies to support researchers and practitioners to meet and share best practices, requirements, challenges and innovative ideas.
A3	Foster **cyber insurance policies** in order to increase welfare of society as a whole and increase cybersecurity preparedness.	Focus on collaborative projects with the countries where the **cyber insurance market** is more developed and adopt them for the EU (e.g., US). Provide the way for researchers to **access available data** (e.g., to reports provided by organisations according to GDPR) about cyber-crime to estimate potential probabilities and impact for reliable risk management. Focus on the projects aiming for **premium discriminating** according to security levels.
A4	Encourage **information sharing** between governmental agencies at national and international levels.	Promote **engagement in the information sharing** initiatives (e.g., like FI-ISAC), providing researchers access to this data. Support the projects that aim to encourage organisations to share their data (rather than just consume).

2.2 Healthcare

The Healthcare sector includes goods and services to treat patients, including hospitals, medical device manufacturers, vendors and the pharmaceutical industry. Digital solutions for healthcare can increase the well-being of millions of citizens and that radically changes the way healthcare services are delivered to patients, if designed purposefully and implemented in a cost-effective way[6].

At the same time, access to data increases the risk of cyber-attacks because many elements are interconnected. IoT Medical Devices also increase the possibilities of cyber-attacks as they are "cloud-connected" via Bluetooth or RFID/NFC. If these devices were to come under attack, the perpetrators could falsify or deactivate the data, and/or modify the release of medicine.

2.2.1 Topics for EU-US collaboration

The following topics were selected for the Healthcare sector:

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

[6] https://ec.europa.eu/health/sites/health/files/ehealth/docs/com2018_233_en.pdf

2.2.2 Challenges

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

2.2.3 Actions

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

2.3 Maritime

Maritime transport serves as the backbone of the world's trade and economic prosperity and its seamless functioning benefits nations and citizens by its efficient shipping of all produce that the globe needs. Current threats to the maritime environment as a whole could disrupt the finely balanced interdependence of today's highly globalized economy, one in which 90% of the total volume of goods is moved by sea and 70% as containerized cargo. Moreover, communications cables that carry 95% of the world's cyberspace traffic lay on the sea-bed.

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. The GPS system is one of the weakest elements of the transportation sector, with potential serious consequences, for example, if cyber-attacks target the container tracking software used by ports or navigation systems. Also there is a risk to life and property if such attacks cause vessel collisions. Systematic delays would cause finance and transportation issues, which in turn could create an impact worldwide on commerce activities.

2.3.1 Topics for EU-US collaboration

The following topics were selected for the Maritime sector:

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

2.3.2 Challenges

- *Different regulations, such as* the GDPR in Europe and the Cybersecurity Information Sharing Act in the US, impose different (and, often, conflicting) requirements on the technology used by the maritime industry as many parts of the overall IT ecosystem are frequently moved from one jurisdiction to another one (e.g., ships and cargo).
- *Heterogeneous environment.* The overall maritime IT ecosystem includes many different parts, which belong to different owners (e.g., ports, coastal guard, ships, cargo, etc.) and have different internal IT systems, different goals, as well as cyber security techniques and practices applied.
- *National and international control.* Maritime research requires to consider the demands of national security and closely cooperation with governmental agencies (e.g., coastal control, navy forces, etc.).
- *Low level of cybersecurity knowledge.* The personnel have very low cybersecurity knowledge and often sees cybersecurity as something that distracts them from the core business. Such an attitude causes resistance to adaptation of additional cybersecurity measures as well as changing the attitude to cyber security practices.

2.3.3 Actions

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

2.4 Prioritization of topics and actions by sector

Topics	Sector	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)	**FINANCE** 	• Agree on and prioritize 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
• 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)	**HEALTHCARE** 	• 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
• 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	**MARITIME** 	• 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 POLICY ACTION AREAS

There are three policy areas that impact bilateral cyber dialogues and research and innovation collaboration between the EU and the US: standards and certification; privacy and data protection; and public-private information sharing. The areas cover the main topics legislators have been working on in recent years, underscoring the fact that both the EU and the US consider these priority areas.

3.1 Key actors in transatlantic cybersecurity policies

Cooperation on these issues requires communicating with the key actors directly involved in crafting new legislation in these areas or updating existing laws. The following table identifies the main EU and US legislative actors and agencies, public and otherwise, involved in the selected cybersecurity policy areas.

Policy Area	EU & US Legislative Actors and Agencies
Standards and certification	**EU Agency for Network and Information Security – ENISA (EU)**: The EU cybersecurity agency ENISA is in charge of preparing EU certification schemes for certain products, services and processes. ENISA helps Member States meet NIS Directive requirements and delivers cybersecurity advice and solutions to Member States and the private sector.[7] **National Institute of Standards and Technology – NIST (US):** NIST is in charge of the NIST Framework, a voluntary guide to help the US´s critical infrastructure operators improve cybersecurity. **Cybersecurity and Infrastructure Security Agency – CISA (US)**: CISA is the key agency involved in building up US cyber resilience. It is works to safeguard government networks and US critical infrastructure.
Privacy and data protection	**European Data Protection Board (EU):** It is part of the GDPR enforcement team. It is made up of 28 data protection authorities from each Member State and has the power to provide guidance on GDPR and rule on important data protection cases. **Data protection authorities in each EU Member State (EU):** They are also in charge of enforcing GDPR in their countries. **European Commission (EU):** The EC reviews the Privacy Shield agreement every year to ensure the EU has been meeting its commitments and assurances with regards to data access for law enforcement and access for national security purposes. **Federal Trade Commission (US)**: It is considered the country´s privacy and data security regulator. It has broad jurisdiction and enforces laws and rules that protect the privacy of health, credit, financial and children, as well as laws that protect consumer information.[8] **States with individual data protection laws (US)**: 48 states have individual data protection laws that require entities to notify individuals if their information has been compromised.[9] **Department of Commerce (US):** It is in charge of reviewing Privacy Shield every year to ensure that the US is meeting its data protection obligations.

[7] European Union Agency for Network and Information Security. About ENISA https://www.enisa.europa.eu/about-enisa

[8] Pahl, Thomas. "Your cop on the privacy beat." Federal Trade Commission Business Blog https://www.ftc.gov/news-events/blogs/business-blog/2017/04/your-cop-privacy-beat

[9] O´Connor, Nuala. "Reforming the U.S. Approach to Data Protection and Privacy." Council on Foreign Relations https://www.cfr.org/report/reforming-us-approach-data-protection

Public-Private Information Sharing	**European Cyber Security Organization - ECSO (EU):** ECSO is an industry group that heads the EC´s contractual Public-Private Partnership (cPPP) in Cybersecurity initiative.[10] **Department of Homeland Security (US):** It oversees the cybersecurity information sharing program between the government and private companies established by the Cybersecurity Information Sharing Act of 2015.

3.2 Comparative analysis between EU and US cybersecurity policies

Each region has a different concept of cybersecurity and privacy and, therefore, shapes its policy using those ideas as a base. The table below summarizes the similarities and differences that emerge in various areas and concepts: laws vs. standards; the work toward harmonizing liability standards; regulation for all sectors vs. regulation for individual sectors; and streamlined enforcement vs. different enforcement actors.

Policy Area	Similarities	Differences
Standards and Certification *EU policies analyzed: NIS Directive, Cybersecurity Act, eIDAS* *US policies analyzed: NIST Framework, Electronic Signatures in Global and National Commerce Act, Uniform Electronic Transactions Act, CISA Act of 2018*	**Improve cyber preparedness**. The NIS Directive and the NIST Framework aim to improve cyber preparedness across the board. **Use the best cybersecurity measures available**. The NIS Directive and the NIST Framework call on entities to use the best available to protect their systems. **No one-size-fits-all solution**. Organizations must employ measures that make sense. **Dedicated agency for cybersecurity focused on protecting critical infrastructures**. The Cybersecurity Act established the EU Agency for Network and Information Security (ENISA) as the region´s cybersecurity agency. The US equivalent is the Cybersecurity and Infrastructure Security Agency (CISA).	**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 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*	**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 establishes clear safeguards for how to handle EU resident data.	**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 streamlined in the US, where

[10] European Cyber Security Organization. "About ECSO." https://ecs-org.eu/about.

Policy Area	Similarities	Differences
services, health, credit reporting and electronic communications	**Spam protection**. The EU and the US recognize that spam is a problem and attempts to cut down on the amount of spam users receive with specific proposed and current regulations.	different agencies regulate different sectors.
Public-Private Information Sharing *EU policies analyzed: NIS Directive, GDPR* *US policies analyzed: CISA Act of 2015*	**Recognized need for information sharing**. With the GDPR and the NIS Directive, the EU establishes the importance of sharing information. In the US, CISA establishes communication channels for the public and private sectors.	**Liability protection**. CISA recognizes that one of the barriers to information sharing is liability and provides liability protection. The NIS Directive also provides this, although GDPR does not.

3.3 Actions

The need to conform to cybersecurity regulations and security industry standards in both the EU and the US, along with the fast-moving technological advances, require policymakers to take action and help build a common ground for EU-US dialogues and collaboration in research and innovation.

Action	What to do	How to do it
A1	**Create an EU-US Cybersecurity Community of Practice (CoP).** The CoP will bring together a group of people who share information, common interest and concerns in cybersecurity, and will act as ambassadors of bilateral dialogues in cybersecurity.	**Organize EU-US co-design workshops** bringing together relevant stakeholders from both sides of the Atlantic. The WS will be held annually, alternative in EU and the US and can be dedicated to specific topics (e.g. blockchain applied to finance and health sectors). **Organize Roundtable briefings**: meetings for EU-US major multipliers to advance cyber certification. Mutual recognition through certification schemes for cybersecurity products could remove administrative and compliance costs.
A2	**Continue to proactively raise awareness** among stakeholders and about the benefits of EU-US dialogues and collaboration in cybersecurity and privacy R&I.	**Fund a new EU-US Coordination and Support Action** to follow the integrated approach of AEGIS, including policy debate and R&I on technologies dealing with the interplay between cybersecurity and privacy across the Atlantic. **Lay the groundwork for a joint funding program in cybersecurity**.
A3	**Cooperation on policies in relation to Data flows.**	**Include prevention, detection, response, repair of cybersecurity incidents** in areas for future cooperation between US and EU. All of these have scope for further cooperation across standards and building capacity.
A4	Bridging work on **Data Privacy by Design (DPbD) and GDPR**.	**Create a framework for DPbD** as a solution that is GDPR compliant would be an excellent EU-US cooperation activity. **Leverage of GDPR in US:** educate end users and industry about implications of GDPR. Collaboration between key actors and agencies from the EU and US.

aegis accelerating EU–US Dialogue in Cybersecurity and Privacy

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