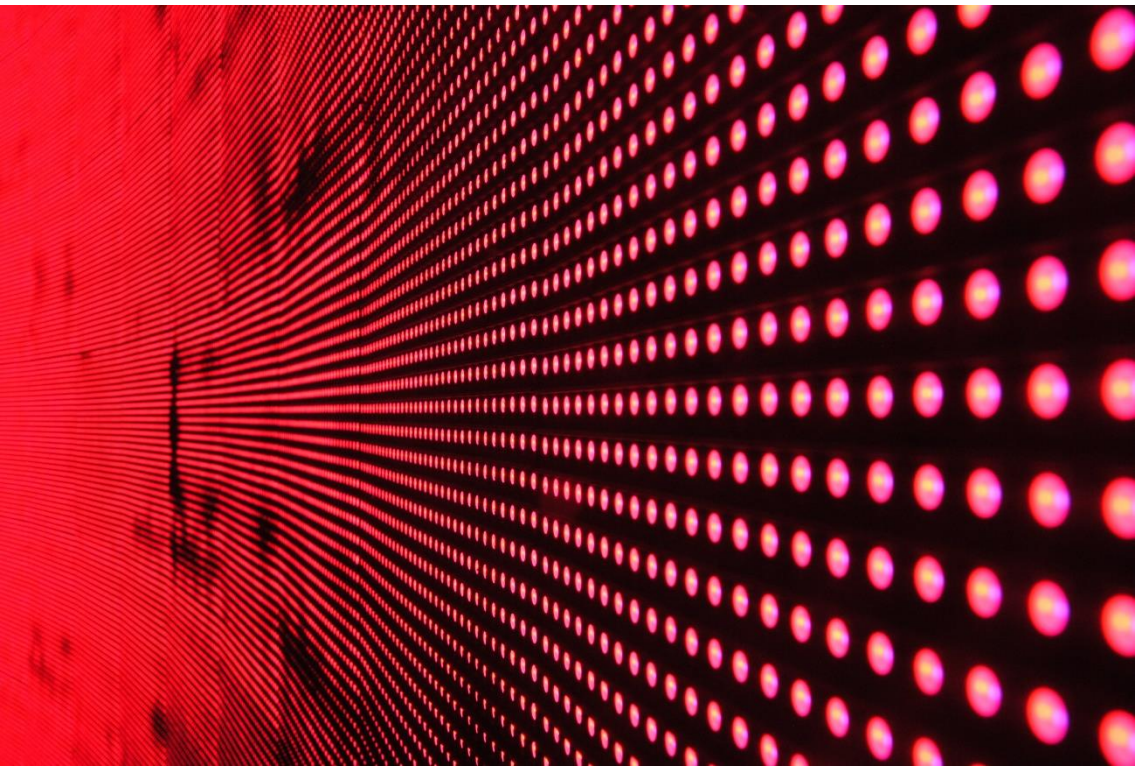
aegis accelerating EU–US Dialogue in Cybersecurity and Privacy



POLICY BRIEF ON CYBERSECURITY POLICY

COMMON GROUND FOR EU-US COLLABORATION

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 EXECUTIVE SUMMARY

The AEGIS project has created this policy brief to capture the current landscape of cybersecurity policies in the EU and the US, two of the biggest players in global cybersecurity policy. It is based on the longer "White Paper on Cybersecurity Policies: Common Ground for EU-US Collaboration" developed by AEGIS. Understanding how each jurisdiction has handled cybersecurity policies is elemental to improving international cooperation in R&I.

The policy brief examines the most current relevant legislation and public policies that can influence future research and innovation collaboration between the EU and the US in the field of cybersecurity and privacy.

Our key findings are as follows:

- **Standards and Certification:** Both jurisdictions agree that it is crucial to improve cyber preparedness and use the best cybersecurity measures available to safeguard systems. No region believes there is a one-size-fits-all cybersecurity solution. The EU has chosen to create laws in this area while the US has opted for voluntary standards.
- **Privacy and Data Protection:** There is consensus that certain types of information must be protected at all costs. Additionally, the EU and the US recognize that spam protection needs to be enshrined in law. In terms of policy execution, the EU has opted for one regulation for all sectors and streamlined enforcement. The US, meanwhile, has various regulations. Enforcement is carried out by diverse agencies.
- **Public-Private Information Sharing:** Through their legislation, the EU and the US emphasize the importance and necessity of public-private information sharing. For years, the US has provided liability protection for organizations to encourage the sharing of information. The EU has recently adopted legislation that provides liability protection, thus the reach and impact of such protections is not yet clear.

2 INTRODUCTION

Both the EU and the US have agreed that it is important to work together on cybersecurity and privacy policy. Given the rapidly changing policy landscape on both sides of the Atlantic and the equally fast moving technological advances, it is important to consider what issues are critical on both sides in order to develop common ground.

Despite the close ties and economic similarities between both jurisdictions, their respective cyber policies have both commonalities and notable differences.

Despite the close ties and economic similarities between both jurisdictions, their respective cyber policies are by no means mirror images.

There are policy areas where the EU has more detailed and developed standards, for instance, and vice versa. This at times makes it a comprehensive analysis difficult. At the same time, it is instructive that not every policy or regulation has an equivalent, as it reflects different approaches to similar concerns as well as different priorities.

Both EU and US stakeholders are interested in knowing what measures the other has taken and why. In areas when there is no equivalent policy, stakeholders must analyze the effects of their current policy. Is it helping researchers and industry or is it hindering them? Would a policy enacted, for instance, in the US also be beneficial in the EU, or vice versa? What policies would make it easier for stakeholders of two of the world´s most significant jurisdictions to work together on cybersecurity R&I?

Based on the similarities and differences of cybersecurity policies in both jurisdictions, we offer recommendations that aim to strengthen EU-US dialogues and to improve R&I cooperation between the EU and the US in the short and long term. These recommendations have the capacity to bring key stakeholders to the table to develop cybersecurity and privacy policies that will allow us to make important strides in R&I.

The document is organized as follows:

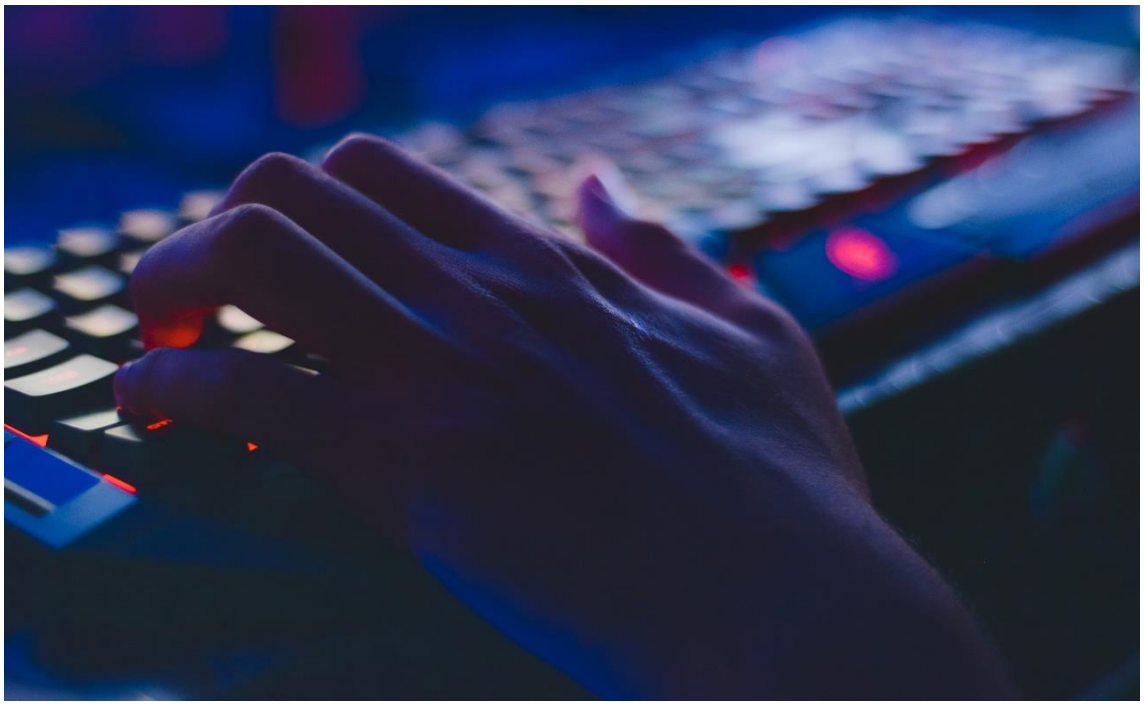
Section 3, "**EU and US cybersecurity strategies**," describes the cybersecurity strategies adopted by each jurisdiction. These are official strategies that have been published in the EU and the US; additional initiatives may be adopted in the future.

Section 4, "**Key cybersecurity policies for effective EU-US collaboration**," lays out the policy areas the document analyzes: standards and certification; privacy and data protection; and public-private information sharing. The AEGIS team chose to analyze these specific groups of policies and regulations based on the major political actions in the EU and the US over the past few years.

Section 5, "**Key actors in transatlantic cybersecurity policies**," describes key actors involved in cybersecurity policy making in both jurisdictions. Meanwhile Section 6, "**Comparative analysis between EU and US cybersecurity policies**,"presents a comparative analysis of EU and US cybsersecurity policies and the actors that craft them.

To conclude, sections 7 ("**Conclusions**") and 8 ("**Policy recommendations**") summarize the key policy points in each area studied and provide a series of recommendations to strengthen EU-US dialogues and enhance collaboration in cybersecurity and privacy R&I.

3 EU AND US CYBERSECURITY STRATEGIES



Although the EU and the US have gone about establishing their cyber preparedness in different ways, both regions share key priorities in their cybersecurity strategies: protecting critical infrastructures, developing a strong cyber defense policy and creating an international cyberspace policy.

3.1 EU Cybersecurity Strategy

The EU outlined its cybersecurity strategy in 2013, titling it "An Open, Safe and Secure Cyberspace." The document presents the EU´s five strategic priorities and its actions in the short and long term. It also details how the jurisdiction will achieve these goals. The priorities are as follows:

- Achieve cyber resilience;
- Drastically reduce cybercrime;
- Develop a common cyber defense policy and develop European Common Security and Defense policy capabilities;
- Develop the industrial and technological resources for cybersecurity; and
- Establish a coherent international cyberspace policy for the European Union that promotes core EU values.

Since the document´s publication, the EU has made significant strides in carrying out its cybersecurity priorities. It enacted the Directive on Security of Network and Information Systems (NIS Directive), which requires Member States and Operators of Essential Services (OESs) to boost their cybersecurity measures. It has also approved the rigorous General Data Protection Regulation (GDPR), a law meant to harmonize all data protection laws in the EU and that imposes strict fines on entities found to be in violation.

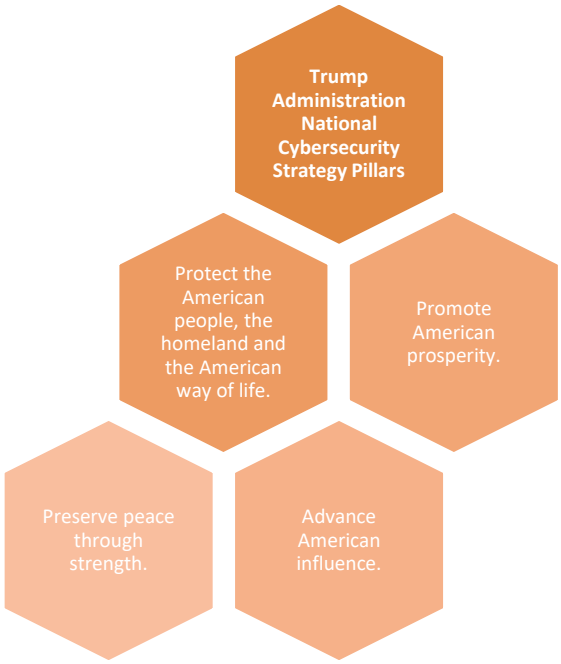
3.2 US Cybersecurity Strategy

It can be difficult to map out cyber capabilities in the US in a comprehensive manner, partly due to the tendency to layer initiatives with agencies. The same is true for the US cybersecurity strategy, which can change under a new president.

In 2018, US President Donald Trump released a national cyber strategy with four pillars. Although the report offered few concrete actions, the initiatives mentioned were considered significant by many in the cybersecurity community. One of those actions was the creation of a Cyber Deterrence Initiative, an effort through which the country plans to build coalitions with other countries to persecute cyber crimes and develop tailored cybersecurity strategies.

The launch of offensive cyber operations was another initiative mentioned in the Trump cyber strategy. This is in sharp contrast to the offensive cyber strategy established by his predecessor, President Barack Obama. Under Obama, the military was required to obtain high-level approval before conducting offensive attacks. Trump eliminated this requirement by rescinding Obama´s Presidential Directive 20.

The following lists the 10 initiatives in Trump´s cyber strategy:



- Secure federal networks and information;
- Secure Critical Infrastructure;
- Combat cybercrime and improve incident reporting;
- Foster a vibrant and resilient digital economy;
- Foster and protect United States ingenuity;
- Develop a superior cybersecurity workforce;
- Enhance cyber stability through norms of responsible state behavior;
- Attribute and deter unacceptable behaviour in cyberspace;
- Promote an open, interoperable, reliable and secure internet; and
- Build international cyber capacity.

The cyber strategy is not the first document in which the Trump Administration focused on strengthening the nation´s Critical Infrastructure. In 2017, Trump signed Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The Executive Order has three goals: increase the cybersecurity of federal networks; improve the cybersecurity of the nation´s critical infrastructure; and improve the nation´s overall cybersecurity.

Although the US has adopted a different strategy under Trump, there are many commonalities between the new strategy and the former Obama strategy. For instance, both considered creating a cyber workforce and protecting the nation´s critical infrastructure to be priorities. It is still too soon to tell what other changes and impacts may result from the new Trump cyber strategy.

4 KEY CYBERSECURITY POLICIES FOR EFFECTIVE EU-US COLLABORATION

There is clear work being done in various cybersecurity policy areas in the EU and US. Some of 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 terms of privacy and data protection, in 2018 the EU enacted the General Data Protection Regulation (GDPR). The US, meanwhile, has acted on public-private information sharing and approved the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) the same year.

The following section provides an overview of key policies and regulations that have been implemented in the EU and US over the past few years. There are various other pieces of legislation that are currently being worked on by policy makers in both jurisdictions through the appropriate legislative processes; a more complete discussion of those is available in the full publication.

4.1 Standards and Certification

One of the key cybersecurity policy areas that has received much attention over the past few years in the US and the EU is standards. In this area, the EU has implemented mandatory legislation that requires Member States and specific organizations to have minimum cybersecurity standards in place. The US has also recognized the importance of minimum cybersecurity standards and created the NIST Framework, a voluntary set of standards to help organizations develop their cybersecurity measures.

The difference in approaches is interesting, and highlights that there are different ways to enact similar policies.

EU Policies

- **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.

- **eID Regulation**

Another aspect of standards and certification the EU has been working on is the eID Regulation, which requires all EU Member States to mutually recognize the national electronic identification schemes used by the bloc´s members. eID aims to allow citizens of one European country to use their national eIDs to securely access online services – such as those provided by public administrations or certain private service providers – provided in other EU countries. All online public services must accept eIDs from other EU countries by September 2018.

US Policies

- **NIST Framework**

In 2014, the National Institute for 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 industry-neutral, meaning that it can be used by a wide range of organizations in different sectors by guiding them through different aspects they should consider as they develop their cybersecurity posture and implementation. It can also be adapted to an organization´s specific needs, which may differ based on industry, size and cybersecurity risk. Additionally, the framework is considered a living document, which means that it may be improved and modified as "technologies and threats evolve.

4.2 Privacy and Data Protection

Privacy and data protection is another policy area that has received much attention over the past few years, particularly in the EU. Nevertheless, in 2018 the US came under pressure to adopt more stringent policies in this area after the Cambridge Analytica scandal, an incident which resulted in the harvesting of data from as many as 87 million Facebook users in 2015, 2.7 million of which were Europeans.

The policies adopted in this area are another example of the different ways to regulate the same area. The EU has decided to take a more streamlined policy approach with the General Data Protection Regulation (GDPR), while the US has opted for a sector and information specific approach.

EU Policies

- **GDPR**

One of the most significant policies that has taken effect in the privacy and data protection area is the EU´s General Data Protection Regulation (GDPR). The GDPR, which was implemented in May 2018, 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.

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.

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. The law had diverse effects on US businesses that operate in Europe. Various publishers blocked Europeans from accessing their websites, citing small European audiences, wariness at the possibility of being fined up to 4 percent of global revenue or €20 million, vague language in the GDPR and concerns about not being full compliant with the law.

US Policies

Unlike in the EU, in the US there is 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, which we will describe below. 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. These laws sometimes overlap and contradict one another. 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 Registrar.

EU-US Policies

- **Privacy Shield**

Another important international agreement tied to privacy and data protection is Privacy Shield, 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 commit to continue doing so. More than 3.300 organizations use Privacy Shield for their transatlantic data transfers, including Facebook, Google, Microsoft, Amazon and Twitter.

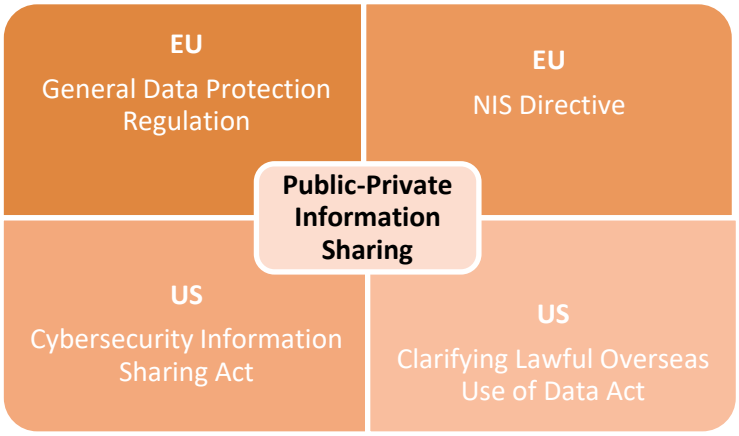
The European Commission and the US Department of Commerce carry out an annual joint review of Privacy Shield to ensure that the US has been meeting its commitments.

4.3 Public-Private Information Sharing

Both the EU and the US have recognized the role of information sharing when it comes to preventing and mitigating cybersecurity attacks. Each jurisdiction has passed significant legislation in this area over the past few years to encourage information-sharing between the public and private sectors. Some laws also encourage collaboration between individual companies in the private sector.

EU Policies

- **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

- **Cybersecurity Information Sharing Act (CISA)**

The US has also been active in the area of public-private information sharing. In order to promote this practice 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 to counteract such threats. It also provides safeguards in order to promote information sharing between private companies and local, state and federal governments as well as between one private company and another private company.

- **Clarifying Lawful Overseas Use of Data Act (CLOUD Act)**

The Clarifying Lawful Overseas Use of Data Act (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.

Notably, the CLOUD Act also gives technology companies the right to challenge the data request if the company feels it violates the laws of the country the data is stored in. 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 the

5 KEY ACTORS IN TRANSATLANTIC CYBERSECURITY POLICIES

The policies mentioned above are crafted and enforced by governmental legislative bodies and agencies. Although policy-making follows similar processes, key differences emerge in the enforcement of laws and creation of policies that do not need legislative approval.

EU Legislative Actors and Agencies	US Legislative Actors and Agencies
European Commission: The EC presents cybersecurity legislative proposals that must be approved by the EU Parliament.	**US President**: The US president sets the nation´s cybersecurity policy and strategy through various mechanisms.
European Parliament: The Parliament considers and approves the legislative proposals introduced by the European Commission.	**US Congress**: The US Congress proposes and approves cybersecurity legislation which later applies to federal agencies, private companies and the general public.
European Council: The Council defines the EU´s political direction and priorities in cybersecurity.	**National Security Council Interagency Process**: The US presidents implements national security and foreign policy decisions using this process.
ENISA: The European Union Agency for Network and Information Security is the bloc´s cybersecurity agency. It aims to harmonize cybersecurity efforts in the EU.	**Department of Homeland Security**: The Department of Homeland Security is the lead agency for asset response activities during a cyber attack.
ECSO: The European Cyber Security Organisation is in an industry-led contractual counterpart of the European Commission that works on the implementation of cybersecurity Contractual Public-Private Partnerships (cPPPs).	**Office of the Director of National Intelligence**: The Office of the Director of National Intelligence is the lead agency for intelligence support and related activities.
Computer Security and Incident Response Teams: Organizations established under the NIS Directive that help deliver a swift and effective response during a cybersecurity incident.	**Department of State**: The Department of State is the main player in international cybersecurity policy.
European Cybercrime Center: Also known as EC3, the European Cybercrime Center is the EU cyber intelligence organization that focuses on cybercrime that affects critical infrastructure.	**Department of Defense:** The Department of Defense is responsible for national cyber defense. It has its own cybersecurity strategy.
J-CAT: The Joint Cybercrime Action Taskforce fights cybercrime on an EU and international level.	**Department of the Treasury**: The Department of the Treasury is in charge of cyber activities and protection for the US financial sector.
Eurojust: Eurojust facilitates legal processes in cross-border cases and investigations.	**Department of Commerce**: The Department of Commerce is responsible for enhancing US cybersecurity awareness and safeguards, protecting privacy and supporting economic and national security.
Computer Emergency Response Team for the EU Institutions, Agencies and Bodies: Also known as CERT-EU, this team works with EU institutions to help facilitate their response to incidents and raising awareness about cyber issues.	**Federal Trade Commission**: The Federal Trade Commission is the nation´s lead cybersecurity enforcement agency.
European Defense Agency: The agency helps Member States build a skilled military cyber defense workforce.	**Department of Justice**: The Department of Justice is the lead US agency for cyber threat response activities.

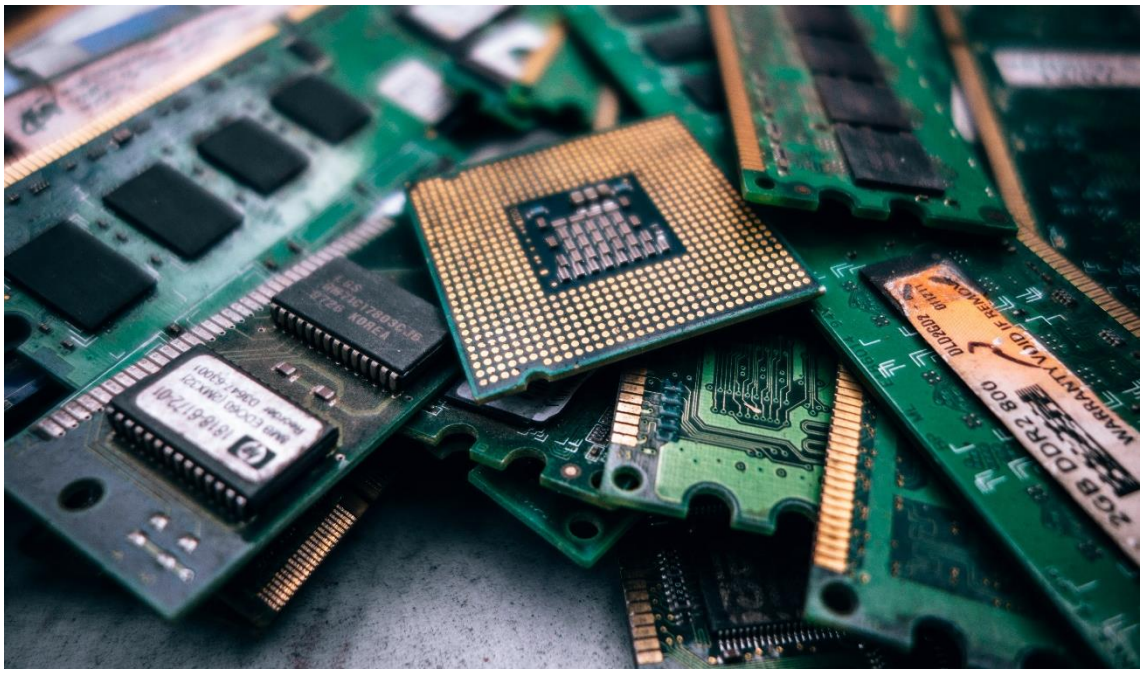
6 COMPARATIVE ANALYSIS BETWEEN EU AND US CYBERSECURITY POLICIES

The biggest differences in EU and US cybersecurity policy can be explained by analysing the most significant laws passed by each region. Some will ask, which approach is better? The question cannot be answered objectively. Each region has a different concept of cybersecurity and privacy and therefore shapes its policy using those ideas as a base.

Policy Area	Similarities	Differences
Standards and Certification	**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.	**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.
Privacy and Data Protection	**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. **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 and current 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 streamlined in the US, where different agencies regulate different sectors.
Public-Private Information Sharing	**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.

Key actors inpolicy making	Similarities	Differences
Various EU and US executive and legislative actors	**Clear recognition that cybersecurity is important**. The executive, legislative and agency bodies of both jurisdictions acknowledge the importance of cybersecurity.	**EU process appears more streamlined**. When compared to the US, there are not many actors involved in the EU policy making process. The US has various processes and entities involved.

7 CONCLUSIONS



Over the last few years, cybersecurity has evolved into a key area of interest between Europe and the US. Both sides have implemented their respective strategies and legislation that shape the transatlantic cybersecurity and privacy policy landscape.

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, which aims to improve critical infrastructure cybersecurity, among others. At the EU level, there is the NIS Directive, which not only applies to EU Member States, but also US companies doing business in the EU.

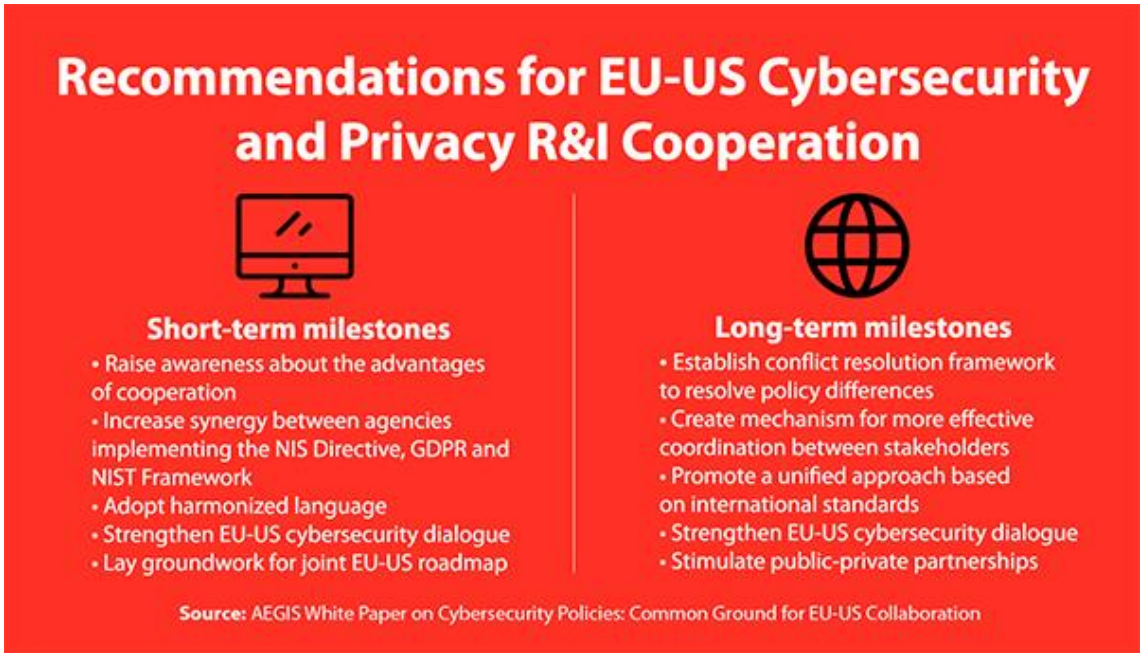
In the privacy and data protection area, the EU and the US have adopted different strategies towards regulation. The EU follows a cross-cutting policy approach through the GDPR, while in the US there is no comprehensive federal data protection law. Instead, the US has opted for a more fragmented and self-regulatory approach affecting certain sectors and types of information.

In terms of public-private information sharing, there is consensus on the role information sharing plays to help prevent and mitigate cybersecurity attacks that also affect private companies. In this regard, 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.

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.

Nevertheless, the comparative analysis of EU and US policies on cybersecurity and privacy demonstrates that in spite of the differences, the approaches to cybersecurity are aligned, which provides common ground for cyberspace harmonization between the EU and the US.

8 POLICY RECOMMENDATIONS



The goals of strengthening EU-US dialogues and improving cooperation on cybersecurity and privacy research and innovation should not be to eliminate policy differences—which besides would be impossible. It should be to develop a set of measures that acknowledge these differences and establish a common ground for collaboration that maximizes the points in common and synergies between EU and US policies and legislation on cybersecurity and privacy.

Based on the analysis of the key cybersecurity policies, we have developed a set of policy recommendations as to how policy makers in the EU and at the federal level in the US can achieve this. These recommendations can be split into two categories: near-term attainable milestones and longer-term goals.

Near-term attainable milestones

1. **Raise awareness among thought leaders and policy makers about the myriad advantages of pursuing deeper connections in the cybersecurity sector.**

   Such awareness can be created through low-cost means including real-time information and insights delivered through various social media. By doing this, policy makers involved in cybersecurity policies in both sides of the Atlantic could benefit from a bottom-up approach and social media engagement to address cybersecurity issues in a more effective way.

2. **Increase synergy and collaboration between the agencies in charge of the NIST Framework and those in charge of the implementation of the NIS Directive and the GDPR.**

   The desired result would be a common framework, standards and practices that would facilitate compliance for companies in the EU and the US. To this end, the use of internet-based connections on a regularly scheduled basis to augment travel to conferences and workshops is a no-cost method that will enhance

cooperation on these issues. This will help create an area of convergence between the EU and the US to implement common policies regarding standards, privacy and data protection.

3. **Adopt a common and harmonised language for stakeholder communication, which will accelerate EU-US collaboration in cybersecurity.**

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 would have the benefit of improving communication and interactions between policy makers in cybersecurity and privacy.

4. **Strengthen EU-US cybersecurity dialogue.**

Existing dialogues should broaden their focus to identify areas for coordination and cooperation in cybersecurity and privacy. Encouragement of meaningful connections among all areas of society, not just limited to experts in the field but extending to commercial enterprises, civil society representatives and elected officials, will expand the demand for closer collaboration. Policy makers involved in EU-US dialogues would further benefit from transatlantic relationships to discuss the future of cybersecurity in Europe and the US and transatlantic cooperation in the field.

5. **Lay the groundwork for a joint roadmap for EU-US collaboration in cybersecurity and privacy R&I.**

The overarching strategy of the AEGIS project is to support policy makers by identifying the most promising areas to sustain transatlantic collaboration and dialogue in cybersecurity and privacy R&I. Foundational work will be developed through significant major multiplier groups that have extensive memberships in diverse groups of society and can begin to inform key stakeholders that opportunities exist to advance transatlantic cooperation in these fields.

Longer-term benchmarks

6. **Establish a framework for resolving conflicts that arise from inevitable differences in policy and regulation.**

Different regulatory attitudes to the global cybersecurity environment can lead to legal conflicts between countries. A framework to address such conflicts when they arise is of paramount importance because conflicts of legal requirements can put companies in a position where complying with the law in one country means breaking the law in another. One example of this conflict can be seen in the French interpretation of the Right to be Forgotten. While France requires search engines to remove Right to be Forgotten cases outside the EU, it does not acknowledge that this could be violating freedom of speech laws in other countries. As a potential remedy, a web-based "clearing house" mechanism could be created that would allow input from a variety of public sector, private industry and civil society voices, which would have the benefit of eliminating as much as possible these types of conflicts.

7. **Establish a new mechanism for more effective coordination between cybersecurity agencies and stakeholders on both sides of the Atlantic.**

One example of this is through the NIS Cooperation Group that could help enhance the sharing of information on threats and best practices at an international level. Such coordination requires better collaboration among key players like the European Commission, ENISA and Member States on the EU side. In the US, coordination would include the agencies involved in cybersecurity policies through the interagency process and establishing closer official and informal relationships with decision-makers to accelerate achievement of mutual objectives. Thus, this coordination mechanism would ensure cooperation and sharing information between cybersecurity related agencies across the Atlantic.

8. **Promote the adoption of a unified approach based on international standards to foster collaboration in cybersecurity R&I across the Atlantic.**

A unified approach will allow EU researchers to develop products and services that have the capabilities to compete in the US market and other international markets. Collaborating on the development of common standards in ICT and ensuring those standards remain voluntary, consensus-based and market-led are critical to this unified approach. With government agencies taking the lead, the private sector, academia and the research communities can ably guide the facilitation of these objectives through leveraging of existing avenues of communication. The feedback from companies engaged in these sectors will be invaluable in achieving competitive advantages that will be of benefit to both transatlantic enterprises and policy makers.

9. **Stimulate public-private partnerships by engaging public organizations and private industry so that they become champions of transatlantic collaboration in cybersecurity.**

Since the private sector is motivated by what serves their customers, engaging civil society and NGO representatives to broaden diversity of opinion and inclusion of disparate perspectives will stimulate company participation. By working together on cybersecurity initiatives, the public and private sectors can both benefit from PPPs, ensuring that cybersecurity developments in the private sector and their policy implications are well understood by policy makers.

aegis accelerating EU–US Dialogue in Cybersecurity and Privacy

Quotation:

When quoting information from this report, please use the following phrase: "Policy Brief on Cybersecurity Policy. AEGIS project."

Consortium:

inmark europa

Consiglio Nazionale delle Ricerche

Waterford Institute of Technology

Hewlett Packard Enterprise

european american chamber of commerce new jersey

THE PROVIDENCE GROUP

RUTGERS

aegis-project.org linkedin.com/company/aegis-project @aegis_cyber