



Guidelines for Innovation Partnerships in Cybersecurity and Privacy for EU-US Collaboration

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.



Copyright © AEGIS Consortium 2017 – 2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
1 INTRODUCTION	5
1.1 Scope and objectives	5
1.2 Target Audience	5
1.3 Deliverable Structure	5
1.4 What's new in the deliverable.....	5
2 METHODOLOGY	6
3 CASE STUDY	9
3.1 DESK RESEARCH.....	9
3.1.1 William and Flora Hewlett Foundation	9
3.1.2 Defense Advanced Research Projects Agency – DARPA.....	10
3.1.3 EU-NATO Agreement	11
3.1.4 Contractual Public-Private Partnership – cPPP	13
3.1.5 Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity – Global EPIC	14
3.1.6 Center for Cybersecurity Policy and Law	15
3.1.7 European Cyber Security Organisation – ECSO.....	15
3.1.8 European Union Agency for Network and Information Security – ENISA 17	
3.1.9 EIT Digital	18
3.1.10 Mind the Bridge – MTB.....	19
3.1.11 Office of Compliance Inspections and Examinations – OCIE	20
3.1.12 United States Coast Guard – USCG.....	21
3.2 IN-DEPT INTERVIEWS.....	22
3.3 ANALYSING DATA	23
3.3.1 William and Flora Hewlett Foundation	23
3.3.2 Defense Advanced Research Projects Agency – DARPA.....	28
3.3.3 EU-NATO Agreement	32
3.3.4 contractual Public-Private Partnership – cPPP	38
3.3.5 Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity – Global EPIC	42
3.3.6 Center for Cybersecurity Policy and Law	49
3.3.7 European Cyber Security Organisation – ECSO.....	54
3.3.8 European Union Agency for Network and Information Security – ENISA 60	
3.3.9 EIT Digital	63
3.3.10 Mind the Bridge – MTB.....	69
3.3.11 Office of Compliance Inspections and Examinations – OCIE	73
3.3.12 United States Coast Guard – USCG.....	79
3.4 BEST PRACTICES.....	83
3.5 GUIDELINES FOR INNOVATION PARTNERSHIP IN CYBERSECURITY AND PRIVACY 86	
3.5.1 Have a strategy to be consistent with certain criteria	88
3.5.2 Multidisciplinary approach to cybersecurity	89
3.5.3 Resilience.....	90
3.5.4 Governance	91
3.5.5 Cooperation and sharing	92
3.5.6 Reputation	93
3.5.7 Innovation.....	94
4 CONCLUSIONS	95
5 REFERENCES	96

LIST OF FIGURES

Figure 1 Hewlett Foundation Large Institutional Activities..... 25
 Figure 2 Hewlett Foundation Cyber Initiative Non-University Grants 26
 Figure 3 EU Member States 33
 Figure 4 Pictures from the EU-NATO agreement signature ceremony 34
 Figure 5 ECISO organization 58
 Figure 6 EIT Digital Strategy 67

LIST OF TABLES

Table 1 Case Study Analysis Results Template 7
 Table 2 Case Studies Best Practices Template..... 8
 Table 3 Best Practice Category Tableau Template..... 8
 Table 4 Case Study Tableau Template 8
 Table 5 Hewlett Foundation Case Study Analysis Results..... 28
 Table 6 DARPA Case Study Analysis Results 32
 Table 7 EU-NATO Agreement Case Study Analysis Results..... 38
 Table 8 cPPP Case Study Analysis Results 42
 Table 9 Global EPIC ecosystem 44
 Table 10 Global EPIC Case Study Analysis Results..... 48
 Table 11 Center for Cybersecurity Policy and Law Case Study Analysis Results 53
 Table 12 European Cyber Security Organization Case Study Analysis Results..... 59
 Table 13 ENISA Case Study Analysis Results 63
 Table 14 EIT Digital Case Study Analysis Results 69
 Table 15 MTB Case Study Analysis Results 73
 Table 16 Office of Compliance Inspections and Examinations Case Study Analysis Results.. 78
 Table 17 United States Coast Guard Case Study Analysis Results 82
 Table 18 Case Study Best Practices Table 84
 Table 19 Best Practices Category 86
 Table 20 Case Studies Table..... 87

EXECUTIVE SUMMARY

Per D3.2 Guidelines for Innovation Partnership in cybersecurity and privacy V1 [1], the objective of this deliverable is to identify good practices for innovation partnerships between organizations from Europe (EU) and the United States (US) to enhance mutual collaboration of most benefit transatlantically. To identify best practices, some additional initiatives and entities have been selected in a wide landscape considering different scopes and areas.

Government agencies, private foundations, political and scientific entities that play a significant role on innovation in cybersecurity and privacy have also been analyzed using a case study methodology approach. Success stories of actual EU-US collaborations already in place have been included in the study.

Projects and initiatives considered are:

Already considered in D3.2

- William and Flora Hewlett Foundation (US)
- DARPA - Defense Advanced Research Projects Agency (US)
- EU-NATO Agreement (EU-US)
- cPPP – contractual Public-Private Partnership (EU)
- Global EPIC – Global ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (EU)

Added in this version

- Center for Cybersecurity Policy and Law (US)
- ECSO - European Cyber Security Organisation (EU)
- ENISA - European Union Agency for Network and Information Security (EU)
- EIT Digital (EU-US)
- Mind the Bridge (EU-US)
- OCIE - Office of Compliance Inspections and Examinations (US)
- USCG - United States Coast Guard (US)

This document outlines the case studies, providing an individual report for each one, and describes the collected (in some cases common) good practices obtained applying the case study methodology.

1 INTRODUCTION

1.1 *Scope and objectives*

This document provides metrics to evaluate practices finalized to improve innovation partnerships throughout EU and US organizations in cybersecurity and privacy, and thus to stimulate industry engagement in cybersecurity and privacy R&I projects.

1.2 *Target Audience*

Industrial and academic research stakeholders interested in establishing partnerships between the EU and the US are the main target audience of this document. Our study represents a guide for identifying best partners based on the good practices of these case studies. The study also serves as a catalyst to improve stakeholder organizations/projects and thus become a partner of interest to other transatlantic entities and to enhance their own internal success.

1.3 *Deliverable Structure*

Before applying case study methodology, a description of its principles is provided in Section 2.

Sections 3, 3.1.11, 0 and 3.4 are dedicated to the phases of the identified methodology and to detailed individual reports about the analyzed case studies.

Section 3.1 includes a summary for each case study that illustrates the salient points of the initiatives and the practices identified as possible good practices for innovative partnerships in cybersecurity and privacy.

Finally, Section 3.5 presents the results of the case study methodology. This section collects good practices and provides guidelines to enable new collaborations between entities in the EU and the US.

1.4 *What's new in the deliverable*

Compared to the information produced in D3.2, this deliverable introduces the following new content:

- Methodology has been enhanced with respect to the one previously proposed (see Section 2);
- To best explain these best practices, we have coordinated some nomenclature to mesh with case studies already considered; and
- We have added some sections to expand results obtained using modified methodology (see Sections 3.4 and 3.5).

2 METHODOLOGY

Per D3.2, we are deploying a **case study methodology** to identify good practices for innovation partnerships between the EU-US.

We conducted an analysis to identify previous studies in which this methodology had already been successfully applied and to elicit from them a methodology that would best meet the aims of our work.

In particular, we identified two examples of similar and successful case studies performed:

- A study on the best practices to enable university-business cooperation in a European context [2]; and
- A research initiative, sponsored by the European Commission and involving many organizations, to find best practices and lessons learned in the management and organization of Large Infrastructure Projects (LIPs) in the transport sector in Europe [3].

We extracted from these examples a common methodology that includes the following steps:

1. **Desk research** (also known as secondary research) - which involves the summary, the collation and/or the synthesis of existing research rather than primary research, in which data are collected from, for example, research subjects or experiments;
2. **In-depth interviews** - with the people working in the foundations/organization to confirm or deny the assumptions or the public retrieved information. People are also involved in order to gather additional material for in-depth analysis of the foundations/organization' initiatives; and
3. **Analyzing data** - Data analysis for these case studies has relied for the most part on qualitative review. Further, analysis has been concurrent with the data collection phase rather than subsequent to it. The principle data analysis method for our case studies is referred to as **OTTR** [4], which stands for
 - a. **Observe** Initial observations are made and tentative hypotheses are formulated;
 - b. **Think** Consideration is made of what additional information must be collected to rule out alternative explanations or confirm initial hypotheses;
 - c. **Test** Additional information is collected through subsequent observation or review; this phase may require interviews with stakeholders or people involved in the observed case; and
 - d. **Revise** Analysis of subsequent observations and review occurs, and initial hypotheses are re-examined.

For this deliverable, we enhanced methodology already used for D3.2 and added another step that consists of:

- a. Assembling all the best practices identified individually in each case study.
- b. Matching the obtained list of best practices with the case studies in order to verify those applicable to each of them.

This analysis includes an iterative process whereby the initial observations are reflected upon and shape subsequent data collection.

The OTTR process continues until the initial hypothesis can be confirmed or until an alternative explanation is required to accommodate new data. In many cases data gathered from case studies are similar and could be easily generalized. In some cases, if data are too differentiated, additional methods are applied until the hypotheses are confirmed or new assumptions are re-examined.

According to these considerations and based on the enhancements introduced in this deliverable, we ultimately identified following steps in order to conduct our work:

- Identify the most relevant initiatives (case studies) for international cooperation in cybersecurity and privacy R&I and potential good practices (success stories) for innovation partnerships between EU and the US;
- For each case study:
 - Observe the key practices which characterize the case study;
 - Provide evidence as basis for each practice and will serve as a good candidate to become a best practice;
 - Complete a one-page summary sheet to compile the salient characteristics of each case study;
 - Elaborate and describe the case study in detail, writing a compendium of each;
 - Define metrics to evaluate the practices. We’ve chosen to follow a qualitative approach to evaluate the identified initiatives. The practices better implemented are those providing tangible evidences;
 - Summarize the observations using a template with having the following structure:

Table 1 Case Study Analysis Results Template

Practice/Activity	Evidence/Outcomes

- Review of best practices and provide a table to compare the case studies analyzed (
-)

Table 2 Case Studies Best Practices Template

Case Studies Best Practices				
		Case Study Name 1	...	Case Study Name n
Best Practice 1	Best practice 1 description			
...	...			
Best Practice n	Best practice n description			

- o Summarize best practices in a table format (Table 3) to define practices to consider;

Table 3 Best Practice Category Tableau Template

Best Practices Tableau	
Best Practice Category 1	Best Practice 1
	...
	Best Practice x
...	...
Best Practice Category n	Best Practice y
	...
	Best Practice z

- Merge the case study tables in a single table (Table 4) to summarize and compare practices and results;

Table 4 Case Study Tableau Template

Case Studies Tableau			
	Case Study Name 1	...	Case Study Name n
Best Practice Category 1			
...			
Best Practice Category n			

- Extract common best practices as result of the analysis; and
- Report the analysis (including the one-page summary and the compendium developed for each case study) and the results, obtained by the methodology application, in the current Deliverable 3.4 "Guidelines for Innovation Partnership in Cybersecurity and Privacy EU-US Collaboration V2."

3 CASE STUDY

3.1 DESK RESEARCH

Each consortium partner has identified one or more organization/foundations with good practices for collaboration between the US and the EU. Each identified organization has then been investigated using online internet research, public governmental information or customer public information (e.g., reports, previous case studies).

Some of these case studies have been chosen as success stories of current EU-US cooperation initiatives already in place. An EU-US agreement is a contract stipulated between two entities belonging to Europe and the United States with the aim to benefit from collaboration in order to overcome common challenges. Taking these parameters into consideration, the Global EPIC is a good example of a truly global partnership, building an ecosystem involving organizations from 10 different countries spanning different continents. Some others have been selected as case studies for their strong contribution to the community and for the considerable impacts they have had or will have.


This section shows the 12 case studies examined. For each of them, a summary sheet is presented. The sheet provides the salient points of the case study and, in particular, the practices implemented that can be good candidates to become enablers for the collaboration between the EU and the US.

3.1.1 William and Flora Hewlett Foundation

<p>Website: www.hewlett.org</p> <p>Name of the case study: Hewlett Foundation</p>	
<p>Background: The William and Flora Hewlett Foundation 's mission is to help people build measurably better lives, concentrating the use of its resources on activities in education, the environment, global development and population, performing arts, and philanthropy, as well as providing grants to support disadvantaged communities in the San Francisco Bay Area.</p>	
<p>Hewlett Foundation's Cyber Initiative: The Hewlett Foundation launched the Cyber Initiative in March 2014. The Hewlett Foundation's Cyber Initiative offers grants to help and support the development of a robust multidisciplinary cybersecurity field that serves the public interest by ensuring the security, stability and resilience of connected devices and a free and open Internet.</p>	
<p>Impact: The Cyber Initiative has been well received by key stakeholders in the government, the private sector, academia, civil society and philanthropy. It has made two sets of grants so far:</p> <ol style="list-style-type: none"> 1. Large institutional grants of \$15 million, respectively, to UC Berkeley, MIT, and Stanford. The grant funded the creation of new cyber policy centers on each campus to educate students in a multidisciplinary fashion with the objective to pursue new policy-relevant research; 	

<p>2. More targeted grants have been provided to individual think tanks, civil society groups and academic centers that have been considered focused on specific policy challenges, outputs and/or individual elements of the foundation’s strategy.</p>
<p>Best Practices:</p> <ul style="list-style-type: none"> • Clear purpose and strategy: The Hewlett Foundation states a purpose for its Cyber Initiative and identifies an accurate strategy for achieving it. The foundation launched the Cyber Initiative in March 2014 and refined its goals and strategy in an updated document [5] in 2016. The official foundation web site dedicates a section to the Cyber Initiative, [20] which is very clear and schematic. It includes goals, ideas, practices and their awarded grants. .In addition, some articles and a “Learn more” section provide in-depth information about cyber initiatives; • Good reputation: The Hewlett Foundation leverages its experience, the quality of grantees, ongoing investments and strategic communication to build a good reputation in order to attract large funders and to promote its initiatives; • Multidisciplinary approach to cybersecurity: The foundation also includes education and policy debates as some of its objectives. Experts from industry, government, think tanks, academia and civil society are involved for achieving the foundation’s objectives; • Make a risk analysis: The Hewlett Foundation included the risks in its strategy paper. It considers the risks related to its strategy and continually produces updated risk documents; and • Tracking progress, evaluating and adjusting strategy in real time: Indicators of progress are identified. One example includes increased amounts of specified outputs, like research, collaborations and funding. Leveraging on an outside evaluator to assess the efforts, the Hewlett Foundation can adjust its strategy in real time as needed.

3.1.2 Defense Advanced Research Projects Agency – DARPA

<p>Website: www.darpa.mil</p>	
<p>Name of the case study: DARPA</p>	
<p>Background: TDARPA’s (Defense Advanced Research Projects Agency) mission is to make pivotal investments in breakthrough technologies for national security. It works within an innovation ecosystem that includes academic, corporate and governmental partners, with a constant focus on US military services, which work with DARPA to create new strategic opportunities and novel tactical options.</p>	
<p>DARPA’s Cyber Initiative: DARPA's objective in cybersecurity is laying a foundation for technologies that will outpace the growth of threats. DARPA’s focus is on creating transformative innovation as opposed to incremental improvements in existing technologies.</p>	
<p>Impact: DARPA has funded more than 20 programs related to cybersecurity so far. Many of them are ongoing at the moment. The full list of initiatives may be found at the following link: https://www.darpa.mil/our-research?ppl=collapse&tFilter=15</p>	

In addition, DARPA launched the Cyber Grand Challenge (CGC) [26] —a competition to create automatic defensive systems capable of reasoning about flaws, formulating patches and deploying them on a network in real time. DARPA hosted the Cyber Grand Challenge Final Event — the world’s first all-machine cyber hacking tournament — in August 2016. CGC was the first head-to-head competition between some of the most sophisticated automated bug-hunting systems ever developed.

Best Practices:

- **Multidisciplinary approach to Cybersecurity:** DARPA has a vibrant ecosystem of innovation within which the agency that operates and is fueled by partners in multiple sectors (university, industry, small business, government, public and media);
- **Sense of mission:** DARPA creates a sense of mission “to prevent and create technological surprise.” People are inspired and energized by the effort to do something that affects the well-being and even the survival of their fellow citizen (and often the citizens of the world), as opposed to the “innovations” that might make a commercial product a bit more scalable;
- **Risk-taking and tolerance of failure:** Openness to new ideas, risk-taking and tolerance of failure are essential elements of DARPA innovation. Proposals submitted to DARPA are reviewed by government experts with advice on specific topics from subject-matter experts both within and outside the government. The Source Selection Board makes recommendations to help the agency decide whether or not to invest;
- **Limited tenure and urgency:** The short tenure and continual rotation of program managers, office directors and deputies is probably one of the single most distinctive features of DARPA’s culture and the most important contributor to continued innovation. The limited tenure means that new people are always being hired, bringing new ideas and their passion for those ideas with them; and
- **Governance:** The freedom to make decisions and take action without having to obtain the permission of managers or supervisors is critical to innovation at DARPA. This does not mean, however, that every innovative idea becomes a program. DARPA has a rigorous approval process for deciding which projects to fund; agency leadership must agree to support a program before millions or tens of millions of dollars are committed to it.

3.1.3 EU-NATO Agreement

<p>Website: http://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf</p> <p>Name of the case study: EU-NATO Agreement</p>	 <p>EUROPEAN UNION</p>
<p>Background: The European Union (EU) is a political and economic union of with 28 Member States that are located primarily in Europe. The EU traces its origins from the European Coal and Steel Community (ECSC) and the European Economic Community (EEC), established, respectively, by the 1951 Treaty of Paris and 1957 Treaty of Rome. The North Atlantic Treaty Organization (NATO), also called the North Atlantic Alliance, is an intergovernmental military alliance between several North American and European states based on the North Atlantic Treaty that was signed on 4 April</p>	

1949. NATO constitutes a system of collective defense whereby its 29 independent member states agree to mutual defense in response to an attack by any external party.

Initiative:

EU Member States and NATO allies established a strategic partnership that takes place in the spirit of full mutual openness and in compliance with the decision-making autonomy and procedures of the organizations and without prejudice to the specific character of the security and defense policy of any members.


Impact:

A stronger NATO and a stronger EU are mutually reinforcing and a deep cooperation between two organizations is necessary in order to enhance new ways of working together and create a new level of ambition. The main reasons to work together are related to the coordination of security, mobilization of a broad range of tools to respond to challenges and a more efficient use of resources. Since July 2016, the EU and NATO have significantly strengthened staff interaction by means of regular meetings, at various levels, including on the preparation of the present set of proposals. Contact points have been established both in the EU and NATO to ensure smooth communication and better cooperation. This staff interaction will continue at regular intervals in order to monitor the implementation of the proposals above, build on those and suggest new directions for progress and report to respective Councils on an annual basis.


Best Practices:

- **Countering hybrid threats:** Boost the ability to counter **hybrid threats**, including by bolstering resilience, working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between staffs;
- **Cybersecurity and defense interoperability:** Cooperating on strategic communication and response. The development of coordinated procedures through respective playbooks substantially contributes to implement efforts;
- **Coherence of intents:** Develop coherent, complementary and interoperable defense capabilities of EU Member States and NATO allies, as well as multilateral projects. Facilitate a stronger defense industry and greater defense research and industrial cooperation within Europe and across the Atlantic;
- **Tracking progress, evaluate and adjust strategy:** Step up coordination on **exercises**, including on hybrid, by developing, as the first step, parallel and coordinated exercises for 2017 and 2018; and
- **Foster cooperation:** Expand coordination on cybersecurity and defense including in the context of EU-NATO missions and operations, exercises and on education and training. Build the defense and security capacity and foster the resilience of partners in the East and South in a complementary way through specific projects in a variety of areas for individual recipient countries, including by strengthening maritime capacity.


3.1.4 Contractual Public-Private Partnership – cPPP

<p>Website: https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp</p> <p>Name of the case study: cPPP</p>	
<p>Background: The cybersecurity contractual Public Private Partnership (cPPP) [5] is a contractual arrangement between the European Union and European Cybersecurity Organization (ECSO). It is part of the EU cybersecurity strategy for enabling and supporting collaboration between the private and public sectors in cybersecurity R&I.</p>	
<p>cPPP's initiative:</p> <ul style="list-style-type: none"> • Encouraging cooperation between public and private entities at early stages of the research and innovation process in order to ensure Europeans have access to innovative and trustworthy European ICT products, services and software with particular attention to security topics like privacy; • Supporting the cybersecurity industry by helping align supply and demand for products and services; • Structuring and coordinating digital security industrial resources in Europe involving a wide range of actors, from innovative SMEs to producers of components and equipment, critical infrastructure operators and research institutes. 	
<p>Impact: The EU will invest €450 million in cPPP via its research and innovation program, Horizon 2020. Cybersecurity market players are expected to invest three times more.</p>	
<p>Best Practices:</p> <ul style="list-style-type: none"> • Clear purpose and strategy: The cPPP was approved in July 2016 and remain in force until December 2020. The acts of the agreements are public. The cPPP objectives are clear and well described. The parties involved in the agreement have specific responsibilities and duties; • Governance: The cPPP has established a board for monitoring, advising and community support. It is the official communication channel between the European Commission and the ECSO association to discuss the Horizon 2020 cybersecurity cPPP work program activities; • Collaboration and sharing: The cPPP organizes public consultation in order to retrieve feedback and suggestions from the stakeholders in order to stimulate cybersecurity dialogue and collaboration outcomes; and • Multidisciplinary approach to cybersecurity: The list of members and substitutes for the cPPP includes large companies, SMEs and associations belonging to different industries and areas. 	

3.1.5 Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity – Global EPIC

<p>Website: www.globalEPIC.org</p> <p>Name of the case study: Global EPIC</p>	
<p>Background: The Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC) was founded to enable the future securely through the development and sharing of new knowledge in the field of cybersecurity – leading to societal, economic and technological impact in a timely fashion. It will be done by building a global community of innovation ecosystems that collaborate on projects and share expertise through an expanding network of diverse organizations.</p>	
<p>Global EPIC’s Cyber Initiative: The Global EPIC initiative was been launched in October 2017 during the 3rd European Cybersecurity Forum, CYBERSEC 2017, in Krakow, Poland. In this initiative, there are 14 global ecosystems co-creating and adopting world-changing solutions to high-impact cybersecurity challenges, both current and emergent. The ecosystems involved come from 10 different countries, reflecting the truly global nature of the partnership.</p>	
<p>Impact: Across the globe, ecosystems that bring together academia, industry and government operate to respond to cybersecurity threats and enable economic development opportunities. The 14 involved ecosystems have largely developed independently, driven by local and national objectives. The leaders of these keystones have become aware that cybersecurity challenges require global paradigm-shifting partnerships and cooperation that reflect regional and local initiatives. Underpinning this perspective is a conscious attempt to ‘glocalize’ – localize the global and globalize the local.</p>	
<p>Best Practices:</p> <ul style="list-style-type: none"> • Clear purpose and strategy: Combining their knowledge, experience and expertise, the Global EPIC ecosystems will together develop innovative solutions, drive knowledge sharing, perform trend analyses and research and also influence and set standards on a global level; • Network of trust: The Global EPIC is a brand new initiative. However, the 14 co-founders have a consolidated experience in the cybersecurity environment; • Multidisciplinary approach to cybersecurity: Education and policy experts from industry, government, think tanks, academia and civil society are involved for achieving the Global EPIC objectives; and • Key areas of activity: Ecosystems within Global EPIC want to share knowledge and experience, contribute to a structured discussion on how to evaluate the resilience of system-of-systems against cyber-attacks, enable horizon scanning, anticipate emerging issues, perform trend analysis and investigate theories of new domains. 	

3.1.6 Center for Cybersecurity Policy and Law

<p>Website: centerforcybersecuritypolicy.org</p> <p>Name of the case study: Center for Cybersecurity Policy and Law</p>	
<p>Background: The Center for Cybersecurity Policy and Law is a nonprofit organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals.</p>	
<p>Center for Cybersecurity Policy and Law Initiative: The Center for Cybersecurity Policy and Law provides a forum for thought leadership for the benefit of those in the industry, including members of civil society and government entities in the area of cybersecurity and related technology policy. It seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices.</p>	
<p>Impact: The Center for Cybersecurity Policy and Law is a nonprofit organization dedicated to improving the cybersecurity ecosystem. The Center hosts several initiatives focusing on a range of critical cybersecurity issues, including</p> <ul style="list-style-type: none"> • Cybersecurity Coalition; • Better Identity Coalition; and • Hardware Vulnerability Project. 	
<p>Best Practices:</p> <ul style="list-style-type: none"> • Clear purpose and strategy: The Center for Cybersecurity Policy and Law hosts several initiatives focusing on a range of critical cybersecurity issues; • Network of Trust: Within its initiatives, the Center for Cybersecurity Policy and Law involves organization leaders from different sectors of the economy, such as health care, technology, telecommunications, fintech, payments and security; • Collaboration and Sharing: One of the center’s main objectives is bringing together leading companies to help develop innovative ideas that improve security, privacy and convenience for all Americans; and • Multidisciplinary approach to cybersecurity: Center for Cybersecurity Policy and Law members include a wide variety of stakeholders such as large company leaders from different sectors. 	

3.1.7 European Cyber Security Organisation – ECSO

<p>Website: ecs-org.eu/</p> <p>Name of the case study: ECSO</p>	
<p>Background: The European Cyber Security Organisation (ECSO) is a fully self-financed non-for-profit organization under the Belgian law established in June 2016. It represents the industry-led contractual counterpart to the European Commission</p>	

for the implementation of the cybersecurity contractual Public-Private Partnership (cPPP).

ECSO Initiative:

The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote and encourage European cybersecurity. It focuses on:

- Fostering the growth of the European Digital Single Market and protecting it from cyber threats;
- Developing the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position; and
- Developing and implementing cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.

Impact:


ECSO members organize Working Groups and Task Forces in order to tackle following priority issues, as defined by the ECSO Board of Directors:

- Standardization, certification, labelling and supply chain management;
- Market deployment, investments and international collaboration;
- Sectoral demand;
- Support to SMEs, coordination with countries (in particular East and Central EU) and regions;
- Education, awareness, training, cyber ranges; and
- SRIA and Cyber Security Technologies.

Best Practices:


- **Clear purpose and strategy:** The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote and encourage European cybersecurity as well as:
 - Promoting Research and Innovation (R&I) in cybersecurity;
 - Proposing a Strategic Research and Innovation Agenda (SRIA) and a Multiannual Roadmap with its regular updates;
 - Fostering demonstration projects and pilots to facilitate bringing innovation to cybersecurity market;
- **Governance:** ECSO is a membership based organization bringing to each of its members a unique opportunity to actively shape the future of cybersecurity strategic research and innovation and build a sustainable market in Europe. All the activities are scheduled based on ECSO Board of Directors directives;
- **ECSO key areas of activity:** ICT Infrastructure, Smart Grids, Transportation, Smart Buildings and Smart Cities, Industrial Control Systems, Public Administration and Open Government, Healthcare, Finance and Insurance are the main area of interest of ECSO; and
- **Multidisciplinary approach to cybersecurity:** ECSO members include a wide variety of stakeholders such as large companies, SMEs and start-ups, research centers, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

3.1.8 European Union Agency for Network and Information Security – ENISA

<p>Website: www.enisa.europa.eu/</p> <p>Name of the case study: ENISA</p>	
<p>Background: The European Union Agency for Network and Information Security (ENISA) is a center of expertise for cybersecurity in Europe. The agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens. Since 2004 ENISA has actively contributed to a high level of network and information security (NIS) within the European Union and to the development of a culture of NIS in society. It has also worked to raise awareness of NIS, thus contributing to proper functioning of the internal market.</p>	
<p>ENISA Initiative: ENISA works closely together with the Member States of the European Union and the private sector to deliver advice and solutions. This includes pan-European cybersecurity exercises, the development of national cybersecurity strategies, cooperation among CSIRTs and capacity building. It also studies secure Cloud adoption; addresses data protection issues, privacy enhancing technologies and privacy on emerging technologies; analyzes eIDs and trust services; and identifies the cyber threat landscape, among others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS.</p>	
<p>Impact: The mid-term ENISA priorities for the next 3 years are following:</p> <ul style="list-style-type: none"> • Anticipate and support Europe in facing emerging network and information security challenges; • Promote network and information security as an EU policy priority; • Support Europe by maintaining state-of-the-art network and information security capacities; • Foster the emerging European network and information security community; and • Reinforce ENISA's impact, by improving the management of its resources and engaging more efficiently with its stakeholders. 	
<p>Best Practices:</p> <ul style="list-style-type: none"> • Clear purpose and strategy: ENISA's strategic objectives are derived from ENISA regulation and inputs from Member States and relevant communities, including private sector; • Good reputation: ENISA is the European Union Agency for Network and Information Security (NIS), established in 2004. As set out in 2013 in its renewed mandate, ENISA has been set up for the purpose of contributing to a high level of Network and Information Security within the Union as well as to growth and employment in Europe; • Key areas of activity: ENISA's activities are focused in three areas: <ul style="list-style-type: none"> ○ Recommendations; ○ Activities that support policy making and implementation; ○ 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU; and • Tracking progress, evaluating and adjusting strategy: Reports presenting the findings and conclusions from the external evaluation of ENISA's core operational activities are provided with the objective of 	

providing ENISA with an evaluation of its performance and an assessment of the possible options for change/improvement.

3.1.9 EIT Digital

<p>Website: www.eitdigital.eu/</p> <p>Name of the case study: EIT Digital</p>	
<p>Background: EIT Digital is a leading European digital innovation and entrepreneurial education organization driving Europe's digital transformation. It delivers breakthrough digital innovations to the market and breeds entrepreneurial talent for economic growth and improved quality of life in Europe. EIT Digital does this by mobilizing a pan-European ecosystem of over 156 top European corporations, SMEs, start-ups, universities and research institutes.</p>	
<p>EIT Digital Initiative: As a Knowledge and Innovation Community of the European Institute of Innovation and Technology, EIT Digital is focused on entrepreneurship and is at the forefront of integrating education, research and business by bringing together students, researchers, engineers, business developers and entrepreneurs. This is done in its pan-European network of co-location centers in Berlin, Eindhoven, Helsinki, London, Paris, Stockholm, Trento, Budapest and Madrid. It also has a hub in Silicon Valley. These centers aim to create a true two-way bridge between the European ecosystem of EIT Digital and the Bay Area ecosystem.</p>	
<p>Impact: EIT Digital invests in strategic areas to accelerate the market uptake of research-based digital technologies focusing on Europe's strategic, societal challenges: Digital Industry, Digital Cities, Digital Wellbeing, Digital Infrastructure and Digital Finance. EIT Digital creates T-shaped entrepreneurial digital talent by focusing on innovation through a blended education strategy that includes a master school, doctoral school and professional school.</p>	
<p>Best Practices:</p> <ul style="list-style-type: none"> • Clear purpose and strategy: EIT Digital invests human and financial resources in key high-potential activities for the development of ICT business and talent in Europe. The investments are clustered in a total of 8 pan-European Innovation and Education Action Lines - portfolios of thematic activities targeting impactful outcomes; • Good reputation: From 2012 to the present, the EIT Digital Accelerator has supported over 270 startups, allowing them to access new markets and gain funding. This is done by providing to the organization a good reputation; • Key areas of activity: The EIT Digital objective is incubation, market uptake and rapid growth of these innovations. As such, the organization focuses its investments on a limited number of innovation areas that have been selected with respect to European relevance and leadership potential - the Innovation Action Lines. EIT Digital currently has five action lines: Digital Industry, Digital Cities, Digital Wellbeing, Digital Infrastructure and Digital Finance; • Multidisciplinary approach to cybersecurity: A key aspect of the Digital Infrastructure Action Line (one of the five EIT Digital action lines) is to catalyze cooperation across the network, computing and security domains. 	


This integration of technologies that typically are only very loosely coupled will create added value. Distributed cloud solutions that are secure and privacy aware for real-time processing based on close integration of networking, computing and security will support new industry segments that are latency sensitive, such as the automotive industry or process industry segments.

3.1.10 Mind the Bridge – MTB

<p>Website: mindthebridge.com</p> <p>Name of the case study: Mind the Bridge</p>	
<p>Background: Mind the Bridge (MTB) is an innovation advisory firm working at the intersection of corporations and startups that provides a suite of advisory services to assist corporations in their open innovation processes, enabling their open innovation drive to be more efficient and more effective. The firm also carries out personalized entrepreneurship programs for international startups and scaleups, immersed in the major innovation ecosystems.</p>	
<p>Mind the Bridge Initiative: Mind the Bridge is a global organization that provides innovation advisory services for corporates and startups. Based in Silicon Valley, with offices in San Francisco, London, Italy and Spain, MTB has been working as an international bridge at the intersection between startups and corporations since 2007. MTB was established in 2007 by then Googler Marco Marinucci, who currently serves as the company's CEO. Italian university professor Alberto Onetti is its chairman. MTB believes that there is societal value in embracing the principles of entrepreneurship as a key accelerator of economies.</p>	
<p>Impact: Mind the Bridge's goal is to foster a sustainable and global entrepreneurial ecosystem. It focuses its programs and activities on bringing startups and corporations together to enhance the growth of all parties as well as to bring new value to enterprises through innovation.</p>	
<p>Best Practices:</p> <ul style="list-style-type: none"> • Clear purpose and strategy: The goal of Mind the Bridge is to foster a sustainable entrepreneurial ecosystem, spur more innovative ideas, and reinvigorate the new venture economy. It does this by providing entrepreneurship education and 360 degrees; • Good reputation: Since 2007, Mind the Bridge has been working as an international bridge at the intersection between startups and corporations. It scouts, filters and works with 1500+ startups a year and supports global corporations in their innovation quest, driving open innovation initiatives that often translate into curated deals with startups; • Key areas of activity: Mind the Bridge activities are focused on: <ul style="list-style-type: none"> ○ <u>Innovation advisory services for corporations:</u> These services are based on education, incentive programs, technology scouting and innovation consulting; ○ <u>Entrepreneurship programs for startups and scaleups:</u> Mind the Bridge carries out a range of activities bringing startups and corporations together during matching events, investing and organizing Startup Europe Comes to Silicon Valley (SEC2SV) and Startup Europe Partnership (SEP). It also has a startup school; 	


- Mind the Bridge foundation:** Mind the Bridge has been running a non-profit foundation since 2007. It was established by Marco Marinucci with the support of a group of entrepreneurs passionate about entrepreneurship education. In 2012, in order to invest in startups with an international soul, Marco Marinucci created a seed investment fund that invests in 6 to 12 startups per year, providing both seed funding and value-added services.

3.1.11 Office of Compliance Inspections and Examinations – OCIE

<p>Website: https://www.sec.gov/ocie/</p> <p>Name of the case study: OCIE</p>	
<p>Background: The Office of Compliance Inspections and Examinations (OCIE) is part of the US Securities and Exchange Commission. The OCIE administers the SEC's nationwide examination and inspection program for registered self-regulatory organizations, broker-dealers, transfer agents, clearing agencies, investment companies and investment advisers.</p>	
<p>OCIE Initiative: OCIE conducts inspections to foster compliance with securities laws, to detect violations of the law and to keep the SEC informed of developments in the regulated community. Among the more important goals of the examination program is the quick and informal correction of compliance problems. When OCIE finds deficiencies, it issues a "deficiency letter" identifying the problems that need to be rectified and monitors the situation until compliance is achieved. Violations that appear too serious for informal correction are referred to the Division of Enforcement. OCIE is organized into several offices and program areas to best support and carry out the mission of the National Exam Program (NEP).</p>	
<p>Impact: OCIE conducts the SEC's National Exam Program (NEP). The NEP's mission is to protect investors, ensure market integrity and support responsible capital formation through risk-focused strategies that: (1) improve compliance; (2) prevent fraud; (3) monitor risk; and (4) inform policy. The results of the NEP's examinations are used by the SEC as a reference for rule-making initiatives. They are also used to identify and monitor risks, improve industry practices and pursue misconduct. NEP staff promote compliance with federal securities laws through exams, outreach, publications and, where appropriate, referrals to the SEC's Division of Enforcement.</p>	
<p>Best Practices:</p> <ul style="list-style-type: none"> Clear purpose and strategy: OCIE publishes its examination priorities annually to improve compliance, prevent fraud, monitor risk and provide a reference for policy. In general, the priorities reflect certain practices, products and services that OCIE believes may present potentially heightened risk to investors and/or the integrity of the U.S. capital markets. Additional priorities may be added in light of market conditions or as OCIE identifies emerging risks and trends; Make a risk analysis: OCIE utilizes a risk-based strategy in order to oversee all of the varying market participants. This happens when an ongoing analysis of root causes harm to investors and markets or when a great risk is identified. Analysis helps set priorities, select potential 	

<p>examination candidates and determine scope of its exams and resource allocation;</p> <ul style="list-style-type: none"> • To be data-driven: Data are used in areas such as risk assessment and exam scoping, planning and execution. Analytics is used to identify potential non-compliance with securities laws, including possible fraudulent behavior. Data is also used to better identify high-risk exam candidates and to more efficiently analyze information during examinations; • Transparency: Publicly sharing certain information about the examination program (priorities, common findings and information about which areas are considered high risk) will ultimately benefit investors by assisting the work of legal, compliance and risk staff at registered entities. Risk alerts, published frequently, helps promote compliance; • Collaboration and sharing: There is a Compliance Outreach Program to promote open communications and coordination on compliance issues among securities regulators and the industry, including investment advisers, broker-dealers, municipal advisers and entities subject to Regulation Systems Compliance and Integrity; • Tracking progress, evaluating and adjusting strategy: OCIE continually assesses its resource deployment and increasingly leverages technology and data in its risk assessment and examination processes; and • Key areas of activity: OCIE embraces innovation and new technology to help benefit the market and investors, to monitor for cybersecurity risks, to help combat cybersecurity attacks and to prevent harm to investors.

3.1.12 United States Coast Guard – USCG

<p>Website: https://www.uscg.mil/</p> <p>Name of the case study: USCG</p>	
<p>Background: The United States Coast Guard (USCG) is a branch of the United States Armed Forces. The Coast Guard is a maritime, military, multi-mission service unique among US military branches for having a maritime law enforcement mission (with jurisdiction in both domestic and international waters) and a federal regulatory agency mission as part of its mission set. It operates under the US Department of Homeland Security during peacetime.</p>	
<p>USCG Initiative: The overall mission of USCG is to ensure the safety, security and stewardship of US waters. The Coast Guard must adapt to the ongoing and rapid advancements in cyber technology. In continuing its history of responding to the ever-evolving maritime needs of the US, the Coast Guard will fully embrace cyberspace as an operating domain.</p>	
<p>Impact: Government systems, including Coast Guard systems, face a mounting array of emerging cyber threats that could severely compromise and limit the service’s ability to perform its essential mission. Adversaries include state-sponsored and independent hacker groups, terrorists and Transnational Organized Crime groups, as well as corrupt, disgruntled and complacent employees (commonly referred to as insider threats). The US is critically dependent on a safe, secure and efficient MTS, which in-turn is highly dependent on a complex, globally-networked system of automated cyber technology.</p>	

Best Practices:

- **Clear purpose and strategy:** The USCG cyber strategy focuses on defending cyberspace, enabling operations and protecting infrastructure. USCG publishes a periodic strategic mid-term plan that serves as a strategic framework;
- **Cybersecurity and defense interoperability:** This refers to asking the owner or operator of a vessel or facility to report activities that may result in a transportation security incident to the National Response Center (NRC), including breaches of security and suspicious activity;
- **Make a risk analysis:** USCG develops, along with the National Institute of Standards and Technology and the National Cybersecurity Center of Excellence, industry segment-specific profiles that serve as risk assessment tools tailored to specific maritime industry segments. The profiles help cyber security and cyber risk management professionals and provide the opportunity to plan for future business decisions;
- **Collaboration and sharing:** The US delegation worked with European Member States and industry representatives to develop the IMO MSC/FAC **Circular Guidelines for Maritime Cyber Risk Management** and MSC Resolution 428(98) Maritime Cyber Risk Management in Safety Management Systems. **Marine Transportation System Cyber Awareness Training** provides basic cyber awareness with a focus on maritime facility and vessel operations;
- **Governance:** The Office of Cyberspace Forces aims to implement the US Coast Guard Cyber Strategy and manages the cyber program. It delivers programmatic oversight and provides direction for the organization. The office also provides training, equipment and information on operational policy for the cyberspace workforce and develops the strategy and policy for enabling operations and protecting MTS infrastructure;
- **Multidisciplinary approach to cybersecurity:** By leveraging its authority and promoting private-public partnerships, the Coast Guard works with the industry to develop and implement measures that will secure critical maritime infrastructure from those who seek to do harm; and
- **Good reputation:** With its operational experience and relationships with federal, state, local, tribal and territorial governments, as well as maritime industry partners, the Coast Guard is the trusted, physical presence in America's ports and waterways.

3.2 IN-DEPT INTERVIEWS

For some case studies it was possible to get in touch with individuals that belong to the initiatives examined. In the case of the cPPP, for example, we have a member of the ECSO in the consortium and we involved him in order to validate our desk research.

When face-to-face interviews have not been possible (for example in William and Flora Foundation) we asked key members of the organization to provide us some specific documentation as reference for our analysis. Participation in speeches or conferences led by members of the organization has been considered in order to reach the same goals (for example the cPPP), leveraging question/answer sessions or direct questions to the speaker. For some others, this phase has been skipped because the progress of the initiative is well documented by public reports and public material (this is the case of the EU-NATO agreement and DARPA).

3.3 ANALYSING DATA

This section includes the compendiums produced for each identified initiative.

3.3.1 William and Flora Hewlett Foundation

Executive Summary

This case study examines the *William and Flora Hewlett Foundation* and puts a special focus on its Cyber Initiative. The Cyber Initiative was launched in March 2014 with an initial funding of \$20 million. This was supplemented with an additional \$45 million for three large grants in November 2014. It has been studied because of its successful approach in facilitating communication among the government, industry and academia. Additionally, the foundation has also been successful in funding international collaboration in cybersecurity and actively pursuing partnerships with leading European foundations, which can feed into the good practices for transatlantic innovation partnerships.

This case study is based on desk research of Cyber Initiative reports [8], Refined Grant Making Strategy [9] and semi structured interviews with key leaders involved this initiative.

Hewlett Foundation's Cyber Initiative

The *William and Flora Hewlett Foundation* [10] is a nonpartisan, private charitable foundation that carries out initiatives in several areas, such as education, the environment, global development and population. It aims to advance education for all, preserve the environment, improve the lives and livelihoods of individuals in developing countries, promoting the health and economic well-being of women, supporting performing arts and some other philanthropy activities. The foundation's mission is to help people build measurably better lives, concentrating the use of its resources on the activities in the areas mentioned above, as well as providing grants to support disadvantaged communities in the San Francisco Bay Area.

In this landscape, with the growing use of the technology in the everyday life, dealing with cyber topics has assumed a fundamental importance since the technology has been included in all aspects of human life. For this reason, the *Hewlett Foundation* made a big effort to investigate the intersections between people, life and technology in order to proactively deal with cyber challenges and propose multidisciplinary solutions for contributing to the healthy development of a more digitalized society. The foundation defined a very precise strategy promoting cyber initiatives and offering grants to support the development of a robust, multidisciplinary cybersecurity field that serves the public interest by ensuring the security, stability and resilience of connected devices and a free and open Internet.

The *Hewlett Foundation* launched the *Cyber Initiative* in March 2014. It released a refined strategy in 2016 [9]. This case study considers the refined strategy, which defines a clear statement of the initiative's purpose:

"To cultivate a field that develops thoughtful, multidisciplinary solutions to complex cyber policy challenges, and by this means catalyze better policy outcomes."

The need for such an initiative emerges because policymakers are finding it ever-more difficult to make informed and sophisticated decisions about cybersecurity policy matters. The time-honored Industrial Age norms and laws seem to be obsolete in the digital era and the complexity of cybersecurity issues is making it very difficult for policymakers to focus on the right problems, balance the competing values or grasp the long-term impacts or trade-offs embodied in policy decisions.

With the term “cyber policy,” the foundation indicates all the aspects that may impact “*the security, stability and resilience of a free and open Internet and connected device,*” which connotes the multidisciplinary aspect of the initiatives, since these topics involve not only the specific technological matters, but also the human aspects (legal, governance, privacy, surveillance, etc.).

In order to satisfy this purpose, the *Hewlett Foundation* will carry out the following activities:

- Build a civil society organization that takes a holistic, multidisciplinary approach to cybersecurity and contributes to a more informed policy debate;
- Educate and expand the knowledge base of existing decision-makers, and educate and empower an emerging generation of cyber policy experts;
- Foster the emergence of a network—comprised of experts from industry, government, think tanks, academia, and elsewhere—that builds trust and promotes collaboration;
- Fund new policy driven research and thought leadership by experts from diverse professional, political and intellectual perspectives; and
- Catalyze additional funding on cyber policy topics from philanthropic, government and private sector sources.

Impact

As a result of the defined actions, the foundation made two sets of grants so far. They are described below:

1. **UC Berkeley** [11] , **MIT** [12] and **Stanford University** [13] each received grants of \$15 million to fund the creation of new cyber policy centers on each campus to educate students in a multidisciplinary approach with the objective to pursue new policy-relevant research. In particular, the objective of these grants is to leverage the leadership and stature of these influencer universities in order to generate policy-relevant research and educate emerging cyber policy leaders. The following chart (Figure 1 Hewlett Foundation Large Institutional Activities) summarizes, for each university, some of the activities carried out to meet these objectives;
2. More targeted grants (detailed in Figure 2 Hewlett Foundation Cyber Initiative Non-University Grants) have been provided to individual think tanks, civil society groups and academic centers that focus on specific policy challenges, outputs and/or individual elements of the foundation strategy. Some examples include NYU [14], the Tax Payer for Common Sense [15] and the Carnegie Endowment [16].



Figure 1 Hewlett Foundation Large Institutional Activities

Through the official website, the foundation provides detailed information about their grants on a dedicated webpage [17] which allows to directly query the grant database and to access to specific reports on charitable activities. The latest report on Direct Charitable Activities, related to 2016, is available on [18].

These reports reveal that the foundation has a strong propensity to involve parties belonging to different areas, including academia, policy makers, universities and research centers in the debate on cybersecurity. This enables not only the sharing of competencies, but also foments collaboration, creating opportunities for individuals to hold meetings, share expertise and build informational resources.

Indeed, the Cyber Initiative within the foundation focuses on how to communicate with policy makers from the perspective of nongovernmental stakeholders, such as industry experts, academia, think tanks, foundations, funding agencies and civil societies. It collaborates with RTI International in *Understanding Demand for Cyber Policy Resources* [19], which outlines recommendations for improving cyber policy supply and demand at the federal level, and includes a checklist for civil society about how to engage with government. The checklist is referenced in different phases of a cyber project or idea, providing recommendations on what to do in the following areas:

- "Before beginning to work on a new idea";
- "Before starting a new project that has been designed";
- "After a project has been started"; and
- "After a project has been completed".

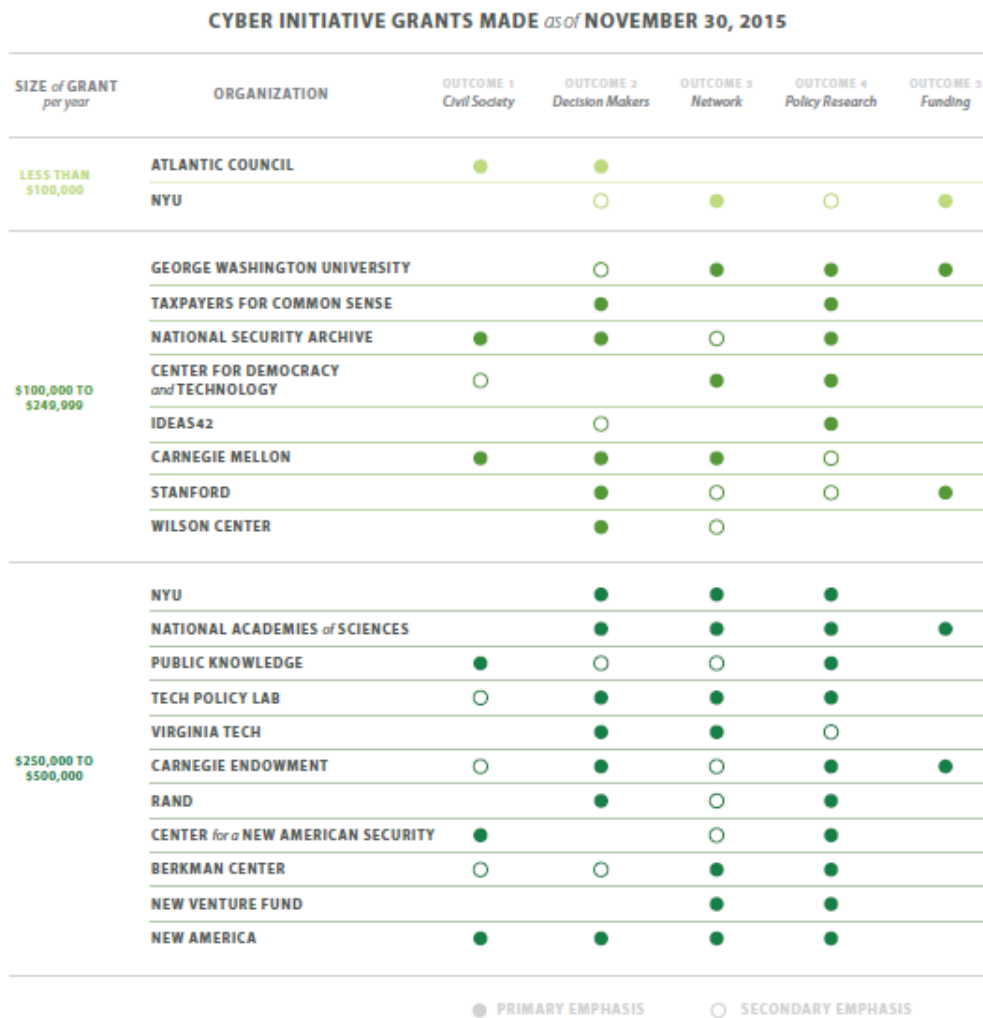


Figure 2 Hewlett Foundation Cyber Initiative Non-University Grants

In this way, the foundation contributes to building a strong multi-disciplinary network of cybersecurity experts, educating existing decision-makers on cybersecurity topics and empowering an emerging generation of cyber policy experts and influencers.

Concretely, the foundation:

- Supports policymakers by funding new policy-driven research written by thought leaders from professional, political and intellectual perspectives; and
- Catalyzes additional funding from philanthropic, government and private sector sources on cyber policy topics.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

The Hewlett Foundation declares a clear Cyber Initiative purpose and identifies an accurate strategy for achieving it. The foundation launched the Cyber Initiative in

March 2014 and refined its goals and strategy in an updated document in the 2016. The official foundation website dedicates a section to "Cyber" [20] which is very clear and schematic, describing goals, ideas and practices and detailing grant activities. Additionally, some articles and a "Learn more" section provide in-depth information about cyber initiatives.

Build effective communication pathways between policy makers and the industry, civil society and the academia

The Cyber Initiative has endeavored to create a pipeline of former military intelligence veterans interested in civil society cyber policy efforts. For example, the foundation provided funding for New America, which became the first US think tank that brings technology, law policy personnel together to work on cybersecurity policy issues.

Good reputation

The Hewlett Foundation leverages its experience, the quality of grantees, ongoing investments and strategic communication to build a good reputation in order to attract large funders and promote its initiatives.

Multidisciplinary approach to cybersecurity

Experts from areas including education, policy, industry, government, think tank, academia and civil society are involved in achieving Hewlett Foundation objectives. Technologists, lawyers, economists, national security practitioners and experts from other disciplines are encouraged to work together.

Carry out a risk analysis

The Hewlett Foundation included the risks in their strategy paper. It considers the risks that arise from the definition of its strategy and updated its risk document.

Tracking progress and evaluating and adjusting strategy in real time

Indicators of progress are identified. For example, increased amounts of specified outputs, like research, collaborations and funding. Leveraging an outside evaluator to assess the efforts, the Hewlett Foundation can adjust its strategy in real time as needed.

Transparency

Grants and direct charity activity reports are public and can be consulted through the website [17].

Case Study Analysis Results

The case study results are summarized in the following table:

Table 5 Hewlett Foundation Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	Have a document of intent that lays out the strategy and the purpose of the initiative.
Build effective communication pathways	New America is the first US think tank that creates a platform for multidisciplinary professionals to communicate with policy makers.
Good reputation	Avoid negative behavior, take on its own responsibilities, build respected partnerships, be reliable and trustworthy.
Multidisciplinary approach to cybersecurity	Involve stakeholders from the government, private sector, academia, civil society and philanthropy.
Carry out a risk analysis	Define a risk plan.
Resiliency	Be ready to recover quickly from emergencies and be flexible when reacting to changes.
Transparency	Be clear and honest. Report and declare activities and expenses.

3.3.2 Defense Advanced Research Projects Agency – DARPA

Executive Summary

This case study examines the *Defense Advanced Research Projects Agency (DARPA)* and puts a special focus on its cyber initiative.

DARPA has led and funded more than 20 programs related to cybersecurity so far. The full list of initiatives [21] may be found at the following link: <https://www.darpa.mil/our-research?ppl=collapse&tFilter=15>.

The consortium has chosen to study DARPA because of its successful experience, which spans more than 50 years, in facilitating communication among university, industry, small business, government and military stakeholders as well as its track record in fomenting and funding international collaboration in cybersecurity.

This case study is based on desk research of cyber initiative reports and semi structured interviews with key leaders involved in this effort.

DARPA's Cyber Initiative

DARPA's [22] mission is to make pivotal investments in breakthrough technologies for national security. DARPA explicitly aims for transformational change instead of incremental advances. However, it does not perform its engineering alchemy in isolation; it works within an innovation ecosystem that includes academic, corporate and governmental partners, with a constant focus on the US military services, which work with DARPA to create new strategic opportunities and develop novel tactical options.

Working with innovators inside and outside of government, DARPA has repeatedly delivered on that mission, transforming revolutionary concepts and even seeming impossibilities into practical capabilities. For decades, this vibrant, interlocking ecosystem of diverse collaborators has proven to be a nurturing environment for the intense creativity that DARPA is designed to cultivate.

Over the past 40 years, DARPA has become ever more connected. These connections have enabled major advances in national security, from pervasive real-time intelligence and communications to optimal logistics. However, increased connectivity has increased the threat of cyber attacks on both military systems and critical infrastructure. Furthermore, modern day software operates within a complex ecosystem of libraries, models, protocols and devices. Ecosystems also change over time in response to new technologies or paradigms as a consequence of repairing discovered vulnerabilities (security, logical and performance-related), or because of varying resource availability and the reconfiguration of the underlying execution platform.

In this regard, DARPA developed a significant effort to investigate the intersections between people, life and technology in order to proactively take on cyber challenges and develop core technology to enable the capability to automatically elicit information from a malicious adversary in order to identify, disrupt and investigate cybersecurity attacks. The agency defined promoting cyber initiatives, leading cyber programs and offering grants to support the development and improvement of the cybersecurity field as part of its mission. Among others, it also identified working on new ways to protect information and systems on Internet as a priority.

DARPA's objective in cybersecurity is laying a foundation for technologies that will outpace the growth of the threat. The agency focuses on creating transformative innovation as opposed to incremental improvements in existing technologies.

Impact

DARPA is recognized for the programs it manages and funds. By stimulating the discussion of new ideas and helping create communities of practice around those ideas, it is also a valuable catalyst for work that companies and universities undertake without direct support. The passionate and visionary ideas of program managers drive DARPA research.

Because of the actions identified, the agency made several sets of grants related to more than 20 funded cybersecurity programs. The complete list of these initiatives and full description of each one is publicly available [21]. A summary of related topics and expected results from these programs are described below:

- Collect data dynamically from mission-critical parts of a network, hunt for threats that evade routine security measures and disseminate protective measures;
- Develop core technology to enable the capability to automatically elicit information from a malicious adversary in order to identify, disrupt and investigate social engineering attacks;
- Develop a system to automatically generate, deploy and enforce configurations of components and subsystems for use in military platforms. These configurations should address system vulnerabilities and minimize attack surfaces while maintaining expected functionality and performance;
- Make currently opaque malicious cyber adversary actions and individual cyber operator attribution transparent by providing high-fidelity visibility into all aspects of malicious cyber operator actions and to increase the government's ability to publicly reveal the actions of individual malicious cyber operators without damaging sources and methods;

- Develop technologies to detect, diagnose and respond to attacks in the cloud; effectively build a 'community health system' for the cloud;
- Develop innovative technologies for detecting and responding to cyber attacks on US critical infrastructure, especially those parts essential to the Department of Defense's mission effectiveness; and
- Address the threat of hidden malicious functionality in COTS IT devices.

Some of the DARPA cyber program elements [23] run during the past 3 years and associated funding with them (all costs are in \$ in millions) are referenced below:

- CYBER SCIENCES (CYS-01)
 - FY15: \$48.178,
 - FY16: \$50.428,
 - FY17: \$45.000;
- CYBER TECHNOLOGY (IT-05)
 - FY15: \$63.891,
 - FY16: \$39.664;
- INFORMATION ASSURANCE AND SURVIVABILITY (IT - 03)
 - FY15: \$11.500,
 - FY16: \$22.000,
 - FY17: \$29.938;
- SECURE INFORMATION AND NETWORK SYSTEMS (CCC-04)
 - FY15: \$2.450;

In addition to the funded cyber programs, DARPA launched the Cyber Grand Challenge (CGC) [24] - a competition to create automatic defensive systems capable of reasoning about flaws, formulating patches and deploying them on a network in real time. By acting at machine speed and scale, these technologies may someday overturn today's attacker-dominated status quo. Making this vision a reality requires breakthrough approaches in a variety of disciplines, including applied computer security, program analysis and data visualization. Anticipated future benefits include:

- Expert-level software security analysis and remediation at machine speeds on enterprise scales;
- Establishment of a lasting R&D community for automated cyber defense; and
- Creation of a public, high-fidelity recording of real-time competition between automated cyber defense systems.

DARPA hosted the Cyber Grand Challenge Final Event — the world's first all-machine cyber hacking tournament — in August 2016 in Las Vegas. Starting with over 100 teams consisting of some of the top security researchers and hackers in the world, DARPA put seven teams against each other during the final event. During the competition, each team's Cyber Reasoning System (CRS) automatically identified software flaws and scanned a purpose-built, air-gapped network to identify affected hosts. For nearly twelve hours, teams were scored based on how capably their systems protected hosts, scanned the network for vulnerabilities and maintained the correct function of software. Prizes of \$2 million, \$1 million, and \$750 thousand were awarded to the top three finishers.

CGC was the first head-to-head competition between some of the most sophisticated automated bug-hunting systems ever developed.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments [25].

Vibrant ecosystem

DARPA has a vibrant ecosystem of innovation within which the agency. It operates and is fueled by partners in multiple sectors (university, industry, small business, government, public, media, etc.).

Sense of mission

DARPA creates a sense of mission “to prevent and create technological surprise.” People are inspired and energized by the effort to do something that affects the well-being and even the survival of their fellow citizen (and often the citizens of the world), as opposed to the “innovations” that might make a commercial product a bit more scalable.

Risk-taking and tolerance of failure

Openness to new ideas, risk-taking and the tolerance of failure are essential elements of DARPA innovation. Proposals submitted to DARPA are reviewed by government experts along with advice on specific topics from subject matter experts from both within and outside the government. The Source Selection Board makes recommendations to help the agency decide whether to invest in a particular initiative.

Limited tenure and sense of urgency

The short tenure and continual rotation of program managers, office directors and deputies is probably the single most distinctive feature of DARPA’s culture and one of the most important contributors to continued innovation. The limited tenure means that new people are always being hired, bringing new ideas and their passion for those ideas with them.

Governance

The freedom to make decisions and take action without having to obtain permission from managers or supervisors is critical to innovation at DARPA. This does not mean, however, that every innovative idea becomes a program. DARPA has a rigorous approval process that it adheres to in order to decide which projects to fund; agency leadership must agree to support a program before millions or tens of millions of dollars are committed to it.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 6 DARPA Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Vibrant ecosystem	The ecosystem is fueled by partners in multiple areas, including university, industry, small business, government, public and media.
Sense of mission	The agency has a clear mission that gives all individuals working at DARPA the chance to be part of shaping the future. People are inspired and energized by the effort to do something that affects the wellbeing of the citizens of the world.
Limited tenure	DARPA constantly reminds all its program managers that time to accomplish important work is limited. This is an impetus to venture into the unknown, get people to put something forward and build the prototypes.
Sense of urgency	Additionally, the agency has a clear perspective about the people who should be hired. Individuals must be fired up to do exciting things, have “their hair on fire” and be determined to achieve something new and important during their short time at the agency.
Carry out a risk analysis	There is a rigorous approval process set up for deciding which projects to fund. Every idea is explored in detail by agency leadership and specific departments.
Governance	People are given the freedom to make decisions and carry out their work as they see fit in order to be effective. They are trusted and expected to trust others. They feel free to do their work in the best way possible, which brings a lot of innovative ideas and approaches to the agency.
Tolerance of failure	Finally, there is a clear message that failure comes from unjustified ambition. Pushing to the edge of what is possible often generates valuable knowledge even though program goals are not always met, information which could be used for future initiatives.

3.3.3 EU-NATO Agreement

Executive Summary

This case study examines the strategic partnership between the European Union (EU) and the North Atlantic Treaty Organization (NATO) and puts a special focus on security and defense initiatives. In this context, cybersecurity has an important role. It must ensure a security interconnection, mobilize a broad range of tools to respond to the challenges and facilitate a more efficient use of resources.

EU-NATO Cyber Initiative

The *European Union* is a political and economic union of 28 member states that are located primarily in Europe. The EU traces its origins from the European Coal and Steel Community (ECSC) and the European Economic Community (EEC), established, respectively, by the 1951 Treaty of Paris and 1957 Treaty of Rome.

The *North Atlantic Treaty Organization*, also called the North Atlantic Alliance, is an intergovernmental military alliance between several North American and European states based on the North Atlantic Treaty that was signed on 4 April 1949.

NATO constitutes a system of collective defense whereby its 29 independent member states agree to mutual defense in response to an attack by any external party.



Figure 3 EU Member States

EU Member States and NATO Allies established a strategic partnership that takes place in the spirit of full mutual openness and in compliance with the decision-making autonomy and procedures of the organizations and without prejudice to the specific character of the security and defense policy of any members.

Closer cooperation between NATO and the EU is key to dealing with current and emerging security challenges. The two organizations are complementary. In the Aegean Sea, NATO is working with the EU closer than ever before. Both organizations continue to work together on missions in Afghanistan and Kosovo. At the Warsaw Summit, NATO aimed for a new level of reciprocal cooperation with the EU, focusing on concrete areas, such as fighting hybrid and cyber threats, supporting partners in defense capacity-building and increasing maritime security.

Sharing strategic interests and facing the same challenges, NATO and the European Union cooperate on issues of common interest and are working side-by-side in crisis management, capability development and political consultations. The EU is a unique and essential partner for NATO. The two organizations share a majority of members and have common values.

NATO and the EU can and should play complementary and mutually reinforcing roles in supporting international peace and security. The allies are determined to make their contribution to create more favorable circumstances through which they will:

- Fully strengthen the strategic partnership with the EU, in the spirit of full mutual openness, transparency, complementarity and respect for the autonomy and institutional integrity of both organizations;
- Enhance practical cooperation in operations throughout the crisis spectrum, from coordinated planning to mutual support in the field;

- Broaden political consultations to include all issues of common concern, in order to share assessments and perspectives; and
- Cooperate more fully in capability development, to minimize duplication and maximize cost-effectiveness.

Fully strengthening this strategic partnership is particularly important in the current security environment, in which NATO and the EU are facing the same challenges to the east and south.



Figure 4 Pictures from the EU-NATO agreement signature ceremony

Impact

A stronger NATO and a stronger EU are mutually reinforcing and a deep cooperation between the two organizations is necessary in order to develop new ways of working together and new level of ambition. The main reasons for cooperation are related to a security interconnection, the mobilization of a broad range of tools to respond to the challenges and a more efficient use of resources.

Because cyber threats defy state borders and organizational boundaries, NATO engages with relevant countries and organizations to enhance international security. Engagement with partner countries is based on shared values and common approaches to cyber defense. Requests for cooperation with the alliance are handled on a case-by-case basis founded on mutual interest.

NATO also works with, among others, the European Union, the United Nations (UN), the Council of Europe and the Organization for Security and Co-operation in Europe (OSCE). The alliance's cooperation with other international organizations is complementary and avoids unnecessary duplication of effort.

The private sector is a key player in cyberspace. Technological innovations and expertise from the private sector are crucial to enable NATO and allied countries to mount an effective cyber defense.

Through the NATO Industry Cyber Partnership (NICP), NATO and its allies are working to reinforce their relationships with the industry. This partnership relies on existing structures and includes NATO entities, national Computer Emergency Response Teams (CERTs) and NATO member countries' industry representatives. Information-sharing activities, exercises, training, education, and multinational smart defense

projects are just a few examples of the areas in which NATO and industry have been working together.

In February 2016, NATO and the EU concluded a Technical Arrangement on Cyber Defense to help both organizations better prevent and respond to cyber attacks. This Technical Arrangement between NCIRC and the Computer Emergency Response Team of the EU (CERT-EU) provides a framework for exchanging information and sharing best practices between emergency response teams.

Since July 2016, the EU and NATO have significantly strengthened staff-to-staff interaction by means of regular meetings, at various levels, including on the preparation of the present set of proposals. Contact points have been established both in the EU and NATO to ensure smooth communication and better cooperation. This staff-to-staff interaction will continue at regular intervals in order to monitor the implementation of the proposals above, build on those and suggest new directions for progress and report to respective councils on an annual basis.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Countering hybrid threats

Since spring 2016, EU and NATO have implemented and operationalized parallel procedures and playbooks for EU-NATO interaction in the areas of situational awareness, cybersecurity, crisis prevention and response and strategic communication.

- **Situational awareness:** Concrete measures were put in place in May 2017 to enhance staff-to-staff sharing of time critical information between the EU Hybrid Fusion Cell and the relevant NATO counterpart, including exchanging the analysis of potential hybrid threats. This established the technical means to allow systematic exchange of information relating to hybrid threats.
- **Strategic communication:** Cooperation has been established between EU and NATO staffs with regard to strategic communication by means of:
 - Intensification of cooperation and sharing of disinformation trend analysis, including through social media targeting the EU and NATO; production, starting at the end of 2016, of an analysis on the above; cooperation in order to improve quality and outreach of positive narrative;
 - Enhancement of mutually reinforcing efforts regarding support for StratCom capabilities of partner countries through coordinated or joint trainings and sharing of platforms;
 - Encouragement of the cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS StratCom division (specifically the Eastern and Southern task forces) including further joint trainings/seminars.
- **Crisis response:**
 - Enhancement of the preparedness, inter alia, by holding regular meetings at staff-to-staff level;
 - Synchronization. This coordination takes into account the EU's crisis response procedures (including the Integrated Political Crisis Response arrangements – IPCR - and NATO's Crisis Response System). It also

considers the two organizations' parallel crisis response activities with the goal of providing coherent support in response to hybrid threats.

- **Bolstering resilience:** The EU and NATO have raised awareness on existing and planned resilience requirements for the benefit of Member States and allies. To that end, as of 2017:
 - Staff contacts have been intensified, including cross-briefings to respective bodies on resilience requirements;
 - Requirements have been assessed, criteria have been established and guidelines have been developed in order to achieve greater coherence between the EU Capability Development Plan (CDP) and the NATO Defense Planning Process (NDPP); and
 - Experts have been made available to support EU Member States and allies upon request. Efforts have also been made to enhancing their resilience, either in the pre-crisis phase or in response to a crisis.

Cybersecurity and defense interoperability

- The EU and NATO have exchanged concepts on the integration of cyber defense aspects into the planning and execution of respective missions and operations to foster interoperability in cyber defense requirements and standards;
- In order to strengthen cooperation on training, as of 2017, the EU and NATO have harmonized training requirements, where applicable, and have open respective training courses for mutual staff participation;
- Both entities have been fostered cyber defense research and technology innovation cooperation by further developing the links between the EU, NATO and the NATO Cooperative Cyber Defense Centre of Excellence. This allows the entities to explore innovation in the area of cyber defense. Considering the dual use nature of cyber domain, the EU and NATO have enhanced interoperability in cyber defense standards by involving the industry where relevant; and
- The EU and NATO have strengthened the cooperation in cyber exercises through reciprocal staff participation in respective exercises, including, for example, Cyber Coalition and Cyber Europe.

Coherence of intent

- There is coherence of output between the NATO Defense Planning Process and the EU Capability Development Plan. This has been pursued through staff to staff contacts and invitations to EU staff to attend NDPP and PARP screening meetings upon invitations by the individual countries concerned;
- Capabilities, developed at a multinational level by allies and Member States, have been made available for both NATO and EU operations;
- Additionally, there has also been an effort to pursue complementarity for multinational projects and programs developed within NATO Smart Defense and EU Pooling & Sharing. These efforts, which are carried out through continued and intensified staff-to-staff contacts, have focused on areas of common interest, such as air-to-air refueling, air transport, satellite communications, cyber defense and Remotely Piloted Aircraft Systems;
- The coherence of multinational efforts has been assured by reflecting multinational projects developed in an EU context, as relevant, in the capability roadmaps supporting NATO defense planning priorities. It has also taken into account multinational projects developed in a NATO context in

deriving priority actions from the EU's Capability Development Plan framework;

- There has also been continued close cooperation between NATO and EU/EDA experts. The field of military aviation has remained one of the focal points of the cooperation, which aims to ensure complementary efforts in the interest of defense and security in Europe, especially when it comes to the development of a military aviation strategy, the implementation of military airworthiness arrangements, Remotely Piloted Aircraft Systems Air Traffic Integration and aviation security including cyber, as well as civil initiatives, such as SES/SESAR; and
- Interoperability has been enhanced through increased interaction on standardization. With the aim to avoid duplication in the development of standards, both organizations have identified projects where standardization related activities could be harmonized.

Tracking progress, evaluating and adjusting strategy

- Parallel and coordinated exercises (PACE) have been implemented as a pilot project for 2017 and 2018. This has been done with NATO serving as the lead through the Crisis Management Exercise 2017 (CMX 17) and will be done with EU as the lead through Multi-Layer Crisis Management Exercise 2018 (ML 18) or other types of exercises in 2018. The exercises include a hybrid element;
- NATO and the EU have staffed experts of the non-leading organization for the respective years to be invited to contribute to the planning and execution of the leading organization's exercise in a spirit of reciprocity;
- Lessons and recommendations have been shared to the extent possible;
- Staff-to-staff exercises have been organized in 2017 in order to test the key modalities already defined in the respective playbooks/operational protocols;
- Training and education have been complemented inter alia through invitations to each other's staff to appropriate events (e.g. workshops, presentations, exercises); and
- NATO, as of 2017, has continued to invite the EU (EEAS and European Commission) to participate in observing its military exercises. The EU will reciprocate accordingly.

Fostering cooperation

- NATO and EU staffs have been fostering cooperation, including on the ground, and focusing on building partners' capacity and resilience, in particular in the Western Balkans and the Eastern and Southern Neighborhoods, which include Georgia, Republic of Moldova, Ukraine, Jordan, Morocco and Tunisia;
- Cooperation and exchange of expertise have been encouraged through respective Centers of Excellence and other relevant training activities and programs in support of partners;
- Possibilities for the EU and NATO to participate in their respective projects and practical partnership programs have been identified; and
- Complementarity of maritime capacity building efforts have been ensured.

Strengthening political dialogue between EU and NATO:

- Regular formal and informal PSC-NAC meetings continue to be organized;
- The practice of sending mutual invitations to relevant ministerial meetings has been pursued and amplified in a balanced manner; and

- Cross briefings to respective Committees and Councils, including on operations, have been strengthened.

Case Study Analysis Results

Since July 2016, the EU and NATO have significantly strengthened staff-to-staff interaction by means of regular meetings, at various levels, including on the preparation of the present set of proposals. Contact points have been established both in the EU and NATO to ensure smooth communication and better cooperation. This staff-to-staff interaction will continue at regular intervals in order to monitor the implementation of the proposals above, build on those and suggest new directions for progress and report to respective Councils on an annual basis.

The case study results are summarized in the following table:

Table 7 EU-NATO Agreement Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Countering hybrid threats	There have been efforts to implement parallel procedures and a playbook for countering hybrid threats.
Cybersecurity and defense interoperability	Both organizations share cyber defense aspects in the areas of operations, missions, training activities and research.
Coherence of intents	The entities take care to avoid negative behavior, take on their own responsibilities, build a respected partnership and be reliable and trustworthy.
Tracking progress, evaluating and adjusting strategy	The EU and NATO are experimenting with collaboration through a pilot project (exercise).
Fostering cooperation	Both organizations exchange expertise, coordinate joint projects and training and cross briefings.

3.3.4 contractual Public-Private Partnership – cPPP

Executive Summary

This case study examines the *contractual Public Private Partnership (cPPP)* signed between the European Union and the European Cybersecurity Organization (ECSO) in July 2016. The agreement remains in force until the end of December 2020. It is part of the EU cybersecurity strategy for enabling and supporting collaboration between the private and public sector. The EU foresees an investment of €450 million in cPPP via its research and innovation program Horizon 2020. Cybersecurity market players are expected to invest three times more.

The analysis is based on desk research of EU reports [27] and on the official arrangement [28]. Some aspects have been validated during a speech dedicated to the cPPP at the launch of Horizon 2020 calls on Secure Societies, which aims to protect the freedom and security of Europe and its citizens" [29]. The launch was led by a member of ECSO.

cPPP Initiative

The European Commission sponsors partnerships in research and innovation in order to address strategic technologies that will sustain growth and jobs in key sectors of the European economy as well as impact society and citizen life.

The cPPP is a contractual agreement (cPPP) between the European Commission and representative industrial associations for key sectors of Europe's economy, which have to join ECSO to participate.

ECSO members include a wide variety of stakeholders across EU Member States, EEA/EFTA Countries and H2020 associated countries, such as large companies, SMEs, startups, research centers, universities, end-users, operators, clusters and associations. The organization also counts on participation from local, regional and national government representatives from Member States.

In terms of this act, the EU and ECSO members will provide funding for research and innovation activities in the most important sectors of the industry. The main goal is to use innovation to generate new business opportunities and thus stimulate the cybersecurity industry.

The agreement lasts seven years during which the parties will implement industry-defined strategic research and innovation initiatives through co-funded projects selected through Horizon 2020 calls for proposals. Under the cPPP, industrial companies, universities, research entities, innovative SMEs and other organizations come together to take on major research and innovation challenges.

ECSO aims to support all types of initiatives or projects that develop, promote and encourage the European cybersecurity industry. The organization, in collaboration with EU and public administrations, is engaged in promoting research and innovation in cybersecurity and privacy.

In order to facilitate bringing innovation to the cybersecurity market, ECSO members are committed to fostering market development and investments in demonstration projects and pilots. The goal of these efforts is to promote and assist in the definition and implementation of a European cybersecurity industrial policy to encourage the use of cybersecurity solutions as well as secure and trustworthy ICT solutions to increase digital autonomy.

ECSO is organized into working groups and task forces, each of them made up of the organization's members. Each of these groups tackles an area identified in the priorities laid out by the ECSO Board of Directors.

The working groups are:

- WG1: Standardization, certification, labeling and supply chain management;
- WG2: Market deployment, investments and international collaboration;
- WG3: Sectoral demand;
- WG4: Support to SMEs, coordination with countries (in particular East and Central EU countries) and regions;
- WG5: Education, awareness, training and cyber ranges; and
- WG6: Strategic Research and Innovation Agenda (SRIA).

Additional details for each working group, including their missions and activities, can be found on the official ECSO website [30].

Impact

The cPPP will have a great impact in several aspects:

- The entities involved in the agreement have tens of millions of people as employees, thus an improvement of in jobs is foreseen;
- A better use of resources is expected since the cPPP board will be responsible for monitoring the activities and Key Progress Indicators that have been established; and
- Europe will become a more attractive location for international companies (including the US) to invest and innovate.

The EU will invest €450 million in the cPPP under its research and innovation program Horizon 2020. Cybersecurity market players are expected to invest three times more. The parties are committed to contribute to meet many EU objectives, including investing 3% of GDP (Gross Domestic Product) in R&D and raising manufacturing's share of the economy to 20% by 2020.

Industries joining the cPPP looks for investments in the development of innovative cybersecurity technologies and the possibility to validate the solutions in key infrastructures and applications. The development of a suitable ecosystem will facilitate innovation and increase investment and awareness for capacity building at a regional, national and EU level. Additionally, it will facilitate the harmonization of the education and training in cybersecurity in order to meet for increased needs in job creation.

In the first 18 months of the cPPP and ECSO, the main achievements were:

- Creation of initial positions for an EU certification framework;
- Support for Cybersecurity Industry Market Analysis (CIMA) [31];
- Investments in the form of initial discussions with banks and insurance companies. There was also support to national bodies to understand and develop investments for startups;
- International cooperation with different countries. There was dialogue with the US. European Commission funded projects to stimulate cybersecurity cooperation between Japan and the US also collaborated in discussions;
- Position paper on the role of SMEs in the cybersecurity ecosystem [32];
- Development of educational initiatives. There was a mapping of educational and professional training courses; mapping of cyber ranges; and the contribution of traineeship offers from ECSO members under the Digital Opportunity Scheme (DG CNECT). In addition, there was also an effort to start tackling gender issues on education and training;
- Definition of research priorities and formalization of the Strategic Research and Innovation Agenda (SRIA [33]); and
- Creation of relationships with other PPPs (BDVA [34], EFFRA [35], 5G [36]).

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

The cPPP was implemented in July 2016 and remains in force until December 2020. The acts of the agreements are public. The cPPP objectives are clear and well described. The parties involved in the agreement have specific responsibilities and duties. Additionally, a very detailed document containing the "Strategic Research and Innovation Agenda" has been drawn up with the priorities for research and innovation for the European cybersecurity industry in the upcoming years.

Governance

The cPPP has established a board for monitoring, advising, community support. It is the official communication channel between the European Commission and the ECSO Association to discuss the Horizon 2020 Cybersecurity cPPP Work Program activities.

The work is organized and distributed via working groups. Each group focuses on specific topics identified by the ECSO board as cPPP priorities. An online application form [37] guides an organization on how to join the community and provides instructions and tools.

Collaboration and sharing

The cPPP organizes public consultations in order to receive feedback and suggestions from stakeholders in order to stimulate cybersecurity dialogue and collaboration. A dense network of events is publicized on the website, events in which members of ECSO participate as speakers or as sponsors. The members of ECSO have committed to the implementation of an "cross-fertilization platform which gathers all main public deliverables from projects, supporting collaboration and clustering along main horizontal issues."

Multidisciplinary approach to cybersecurity

The list of members and substitutes of the cPPP includes large companies, SMEs and associations belonging to different industries and areas.

Categories are defined for members:

- *Large companies*: developing and/or manufacturing cybersecurity solutions or providing services;
- *National and European organizations / associations*: representing interests at the national, European and international level;
- *SMEs*: Associations composed only by SMEs, startups, incubators and accelerators.
- *Users / operators of national public administrations or private companies (large or SMEs)*: directly represented.
- *Regional / Local public administrations*: regional / local clusters of public / private legal entities with local economic / ecosystem development interests;
- *Public administrations at the national level*;
- *Research Centers, academia and universities*: associations composed only by research centers, academia or universities; and
- *Others* (financing bodies, insurances, consultants, etc.).

Case Study Analysis Results

The case study results are summarized in the following table:

Table 8 cPPP Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	The cPPP has an act to describe the terms of the agreement, including the purpose, goals, responsibilities and governance structure.
Governance	The initiative nominates a board for monitoring, advising, tracking activities and mobilizing community support.
Collaboration and sharing	The cPPP organizes public consultation for collecting feedback and suggestions from stakeholders in order to stimulate cybersecurity dialogue and collaboration. It also includes information sharing and participating or sponsoring public conferences and events as part of its objectives.
Multidisciplinary approach to cybersecurity	The list of members and substitutes of the cPPP includes large companies, SMEs and associations that belong to different industries and areas.

3.3.5 Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity – Global EPIC

Executive Summary

This case study examines the *Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC)*. This cyber initiative was launched in October 2017 during the 3rd European Cybersecurity Forum, also known as CYBERSEC 2017, in Krakow, Poland.

Together, Global EPIC ecosystems (combining their knowledge, experience and expertise) are going to develop innovative solutions, drive knowledge sharing, perform trend analyses and research and influence and set standards on a global level.

This case study is based on the terms of reference of Global EPIC [38].

Global EPIC Initiative

The *Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity* [39] is a global community of innovation ecosystems that collaborate on projects and share expertise through an expanding network of diverse organizations.

The purpose of Global EPIC is to co-create and adopt world changing solutions to high-impact current and emergent cybersecurity challenges through the development and sharing of new knowledge in the field.

Cybersecurity threats are a global challenge that disrupt local modern living that are continuously evolving. Everyday there is news related to an attack, which suggests that the current cybersecurity approaches are failing.

Across the globe, ecosystems that bring together academia, industry and government operate to respond to cybersecurity threats and enable economic development opportunities. These ecosystems have largely developed independently and are

driven by local objectives. Nowadays, their leaders are becoming aware that cybersecurity challenges require global paradigm shifting partnerships and cooperation that reflect regional and local imperatives. Based on this awareness, Global EPIC focuses on both co-creating globally and benefitting locally, or attempting to *glocalize*: localize the global and globalize the local.

The Global EPIC initiative has been launched in October 2017 [40]. This case study considers the initial value generation initiatives of Global EPIC that are organized and described below:

- **Network** Each organization provides resources and processes of potential value to other keystones that are part of EPIC. These offerings include:

 - soft landing services;
 - connections to potential customers, multinationals, expert advisors in intellectual property, legal services and financial matters;
 - shared operational tools and facilities;
 - ecosystem-specific information (e.g. common language standards, professions, qualifications); and
 - knowledge and experience.
- **Projects** Global EPIC enables community-generated solutions to domain specific challenges, such as multidisciplinary or fundamental problems;
- **Talent** Global EPIC creates development programs to enhance the skill sets and knowledge of individuals operating in specific scenarios;
- **Exchange** Global EPIC enables matchmaking between otherwise disparate ecosystem entities. Examples include:

 - Connecting an enterprise in one ecosystem with a specific mentor in another ecosystem, and
 - Enabling ecosystem enterprises to offer products and services globally thereby accelerating revenue growth.
- **Evaluation** Global EPIC contributes to a structured discussion on how to evaluate the resilience of system-of-systems against cyber attacks;
- **Content** Global EPIC enables content sharing across an organization's ecosystem. Examples of such content include datasets, localized social networking feeds and journal articles;
- **Emerging** Global EPIC enables horizon scanning, anticipation of emerging issues, trend analysis and investigation of theories of new domains;
- **Advocacy** Global EPIC uses its global reach and status to advocate for and raise awareness of causes, policies and recommendations aligned with its general purpose of co-creating and adopting world changing solutions to high-impact cybersecurity challenges;
- **Investment** Global EPIC strives to become an engine behind generating a global framework program for research and innovation and play a major role in defining budget allocation mechanisms and prioritization; and

- **Standards** Global EPIC acts in a synchronizing role (using the assets and expertise of its members) in attempting to standardize our understanding of cybersecurity.

Impact

As already stated, the 14 ecosystems involved in the initiative, driven by local and national objectives, have largely developed independently in order to respond to cybersecurity threats and enable economic development opportunities. Currently, these ecosystems have become aware that the challenges of cybersecurity require global paradigm-shifting partnerships and cooperation that reflect regional and local imperatives.

Global EPIC aims to have 50 organizations in its cybersecurity ecosystem by October 2020. The following table provides Global EPIC ecosystem reference information:

Table 9 Global EPIC ecosystem

 ISRAELI CYBER INNOVATION ARENA	Cyberspark (http://cyberspark.org.il/)
	Centre for Secure Information Technologies (http://www.csit.qub.ac.uk/)
	The Hague Security Delta (https://www.thehaguesecuritydelta.com/)
	Global Cybersecurity Resource – Carleton University (https://cugcr.com/lce/index.php)
	The Canadian Institute for Cybersecurity (CIC), University of New Brunswick (http://www.unb.ca/cic/)
	CyberTech Network (http://cybertechnetwork.org/)
	The Kosciuszko Institute (http://www.ik.org.pl/en/)
	Politecnico di Torino (http://www.polito.it/?lang=en)
	INCYDE (http://www.incyde.org/)
	Cyber Wales (https://cyberwales.net/)

	bwtech@UMBC (http://www.bwtechumbc.com/)
	Procomer (https://www.procomer.com/en/)
	Innovation Boulevard (http://www.innovationboulevard.ca/)
	LSEC (https://www.leadersinsecurity.org/)

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

Combining their knowledge, experience and expertise, the Global EPIC ecosystems will develop innovative solutions, drive knowledge sharing, perform trend analyses and research and influence and set standards on a global level.

For instance, a driver of Global EPIC knowledge sharing is their portal where:

- Institutions such as academia (e.g. universities), innovative industry (e.g. startups, local businesses, multinationals) and government (regional through to national) focused on innovation activities for economic benefit can join [41];
- Additionally, there are currently posted alerts related to cyber attacks as well as activities and success stories of Global EPIC founders' ecosystems.

As the world becomes more and more social, Global EPIC has opened several accounts on mainstream social networks, including:



<https://www.facebook.com/Global-EPIC-120069531996204/>



<https://twitter.com/GlobalEPIC>



<https://www.instagram.com/globalepic/>

Network of trust

Global EPIC is a new initiative but the 14 co-founders have a consolidated experience in the cybersecurity environment, which is described below:

<i>Cyberspark</i>	Cyberspark is a joint venture of the Israeli National Cyber Bureau in the Prime Minister's Office, the Beer Sheva Municipality, the Ben Gurion University of the Negev and leading companies in the cybersecurity industry.
<i>Centre for Secure Information Technologies</i>	The Centre for Secure Information Technologies is part of the Institute of Electronics, Communications and Information Technology (ECIT). This unique environment encourages collaboration among academics, researchers, engineers, industry and government to accelerate the results of cyber and physical security research through to commercial application.
<i>The Hague Security Delta</i>	The Hague Security Delta is a cluster located in The Hague in The Netherlands, where businesses, governments, and knowledge institutions work together on innovations in cybersecurity, focusing on national and urban security, protection of critical infrastructure and forensics.
<i>Global Cybersecurity Resource – Carleton University</i>	The Global Cybersecurity Resource – Carleton University is a non-profit organization established and managed by the Technology Innovation Management program of Carleton University. It works on equipping high growth cybersecurity and cybersecurity-differentiated companies with the skills, resources and connections required to be successful.
<i>The Canadian Institute for Cybersecurity (CIC), University of New Brunswick</i>	The Canadian Institute for Cybersecurity is part of the University of New Brunswick in Canada. It's a comprehensive multidisciplinary training, research and development and entrepreneurial unit that draws on the expertise of researchers in the social sciences, business, computer science, engineering, law and science.
<i>CyberTech Network</i>	The CyberTech Network is a global cybersecurity and Internet of Things (IoT) network ecosystem that provides cybersecurity and IoT resources, strategic programs and thought leadership events across the US. In partnership with national and local organizations, CyberTech stimulates innovation and advances the adoption of cyber and IoT technologies for the economic and social benefit of the US.
<i>The Kosciuszko Institute</i>	The Kosciuszko Institute is a leading, non-governmental and non-profit think tank and research institute that acts in the interest of the socio-economic development and security of Poland as a proactive member of the European Union and NATO.

<i>Politecnico di Torino</i>	Politecnico di Torino is one of the most important universities in Europe for engineering and architecture studies. The university is strongly committed to collaboration with the industry. Politecnico is a research university that participates at the highest levels of international scientific research.
<i>INCYDE</i>	INCYDE is an institution created by various chambers of commerce dedicated to the promotion and teaching of entrepreneurship. It aims to improve the qualifications of entrepreneurs and to create and consolidate companies.
<i>Cyber Wales</i>	Cyber Wales is an ecosystem that brings together academia, industry and government activities.
<i>bwtech@UMBC</i>	Bwtech@UMBC is a community that brings together research, entrepreneurship, business leads, prospective clients and economic development in Maryland. It is a place full of like-minded businesses on the forefront of innovation. This community is a center of innovation for businesses in all different stages of development.
<i>Procomer</i>	Procomer is the institution in charge of promoting the exportation of Costa Rican goods and services throughout the world.
<i>Innovation Boulevard</i>	Innovation Boulevard is an agile partnership of health, business, higher education and government creating new health technologies to improve lives.
<i>LSEC</i>	LSEC is an international IT and Information Security cluster. It is non-profit organization that promotes information security and expertise in Europe. Founded by the University of Leuven and supported by the European Commission FP7 program, LSEC leads a PAN European private partnership that interacts with public institutions. LSEC connects security experts, research institutes and universities, government agencies, end users, funding bodies and technical experts who are driving European research agendas.

Multidisciplinary approach to cybersecurity

As already stated in the previous section, experts from areas such as education, policy, industry, government, think tanks, academia and civil society are involved in Global EPIC in order to achieve the defined objectives.

Each ecosystem has to provide personnel, financial and other resources to:

- Constructively contribute to the Global EPIC purpose; and
- Leverage Global EPIC to provide value to its local economy.

Global EPIC operates as an ecosystem linking keystone organizations that anchor cybersecurity ecosystems globally. It is governed by a decision-making board composed of representatives of each keystone organization.

One of the keys to Global EPIC’s success is the creation of a community that adheres to its purpose and underlying globalization ethos. The value generation initiatives described above are a means for building the community. The community will be drawn from the keystone organizations and can include, for example, companies, researchers, mentors and consultants.

Moreover, regular face-to-face meetings, fundamental to community building, will be held at locations that take into consideration the geographic posture of Global EPIC. Annually, Global EPIC will hold a symposium (potentially co-located with another major event such as board meetings) that focuses on institutional contributions and challenges.

Key areas of activity

Ecosystems within Global EPIC want to share knowledge and experience, contribute to a structured discussion on how to evaluate the resilience of system-of-systems against cyber-attacks, enable horizon scanning, anticipate emerging issues, analyze trends and investigate theories of new domains.

In order to do that, each ecosystem has to actively participate in network building and provide resources and processes of potential value. Global EPIC, meanwhile, has to enable community-generated solutions and create development programs to enhance the skill sets and knowledge of individuals operating in specific scenarios.

Moreover, matchmaking between otherwise disparate ecosystem entities as well as generating a global framework program for research and innovation are fundamental factors for the success of Global EPIC. Having a major role in defining budget allocation mechanisms and prioritization are also crucial.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 10 Global EPIC Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	Global EPIC has a document of intent that declares the strategy and the purpose of the initiative.
Network of trust	The initiative avoids negative behavior, take on its own responsibilities, builds respected partnership and is reliable and trustworthy.
Multidisciplinary approach to cybersecurity	Global EPIC involves stakeholders in the government, private sector, academia and civil society. Additionally, the organization defines a clear and thin management structure in order to achieve stated goals.
Key areas of activity	The organization has also defined a value generation initiative plan.

3.3.6 Center for Cybersecurity Policy and Law

Executive Summary

This case study examines the **Center for Cybersecurity Policy and Law**, a nonprofit organization that develops, advances and promotes best practices and educational opportunities among cybersecurity professionals in order to improve the cybersecurity ecosystem.

The center is engaged in several initiatives focused on a range of critical cybersecurity issues including:

- Cybersecurity Coalition;
- Better Identity Coalition; and
- Hardware Vulnerability Project.

This analysis is based on desk research and on information found on the center's website [42].

Center for Cybersecurity Policy and Law Initiative

The *Center for Cybersecurity Policy and Law* provides a forum for thought leadership to benefit the industry, members of civil society and government entities in the area of cybersecurity and related technology policy.

It seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies and groups of all sizes to take steps to improve their cybersecurity practices.

Activities are focused on many initiatives that include:

- **Cybersecurity Coalition** [43]
that is an organization founded by several leading companies in the cybersecurity industry leading in order to offer their expertise on critical policy issues;
- **Better Identity Coalition** [44]
that is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication; and
- **Hardware Vulnerability Project** [45]
that is a new project that has already produced some result such as the development of processes, policies and practices with a greater focus on software rather than hardware.

Impact

As already stated before, The *Center for Cybersecurity Policy and Law* is a nonprofit organization dedicated to improving the cybersecurity ecosystem. The center hosts

several initiatives focused on a range of critical cybersecurity issues, including the ones described below, and organize many events and symposiums related to cybersecurity in order to enhance awareness on this strategic topic.

Cybersecurity Coalition

Launched in February 2016, the Cybersecurity Coalition works with leaders to develop consensus-driven policy solutions that promote a vibrant cybersecurity ecosystem, support the development and adoption of innovations and encourage organizations to take steps to improve their cybersecurity.

In order to achieve its mission, the coalition monitors and addresses interactions and intersections between government entities, researchers and vendors. It also promotes its mission to the US Congress, federal agencies, international standards bodies, industry self-regulatory programs and relevant policymaking venues.

The coalition is focused on several active and critical policy issues that require close alignment and coordination to protect the vital interests of the cybersecurity products industry, including:

- Promoting responsible vulnerability research and disclosure;
- Promoting effective privacy processes within cybersecurity policy;
- Establishing government requirements for agency systems;
- Increasing information sharing and threat intelligence; and
- Promoting sound cybersecurity practices in government at all levels.

Better Identity Coalition

Launched in February 2018, the Better Identity Coalition is a nonprofit organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication.

The coalition released a report that outlines a comprehensive policy agenda for improving the privacy and security of digital identity solutions called **Better Identity in America: A Blueprint for Policymakers** [46] that highlights the following key initiatives:

- Prioritize the development of next-generation remote identity proofing and verification systems;
- Change the way people in the US use their Social Security Number;
- Promote and prioritize the use of strong authentication;
- Pursue international coordination and the harmonization of identity standards; and
- Educate consumers and businesses about better digital identity solutions.

The focus of the coalition for 2018 is on following priorities:

- Engagement of government in order to identify when and where the coalition's input can be most timely and impactful;
- Definition of challenges by means of "first-generation" identity verification and authentication tools;
- Identification of regulatory, policy or technical barriers that inhibit companies or government from improving these tools; and

- Development of new policies and initiatives in order to help both government and industry deliver next-generation identity solutions more secure and better for privacy and customer experiences.

Hardware-Centric Coordinated Vulnerability Disclosure Practices Initiative

Launched in April 2018, the initiative brings together key stakeholders from across the technology sector to identify the needs and state of the hardware ecosystem, detect possible gaps in disclosure policy and practice and assess options for future improvements.

While this initiative has just begun, a few key areas and themes have already emerged. Among which the most relevant is the following: industry vetted processes, policies and practices that were developed with a greater focus on software than hardware.

In order to address above mentioned topic, the project has been structured in 3 phases:

- Detailed comparative analysis of existing policies and practices;
- Survey of the partners involved in the patching process to understand the views of different industry segments dependent on hardware components; and
- Recommendations.

This means bringing together the researchers that find vulnerabilities and key stakeholders from all of the groups involved in the patching and disclosure processes in each of these phases. Additionally, it also means talking to consumer groups, academics and those who have helped design and run the software and hardware patching and disclosure processes in the past.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

The Center for Cybersecurity Policy and Law has several initiatives focusing on a range of critical cybersecurity issues.

Among those initiatives, the following stand out:

- The **Cybersecurity Coalition** works with leaders to develop consensus-driven policy solutions that promote a vibrant cybersecurity ecosystem, support the development and adoption of innovations and encourage organizations to take steps to improve their cybersecurity;
- The **Better Identity Coalition** is focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication; and
- The **Hardware-Centric Coordinated Vulnerability Disclosure Practices Initiative** that brings together key stakeholders from across the technology

sector to identify needs and circumstances of the hardware ecosystem, possible gaps in disclosure policy and practice, and options for future improvements.

Network of Trust

Within its initiatives, the Center for Cybersecurity Policy and Law involves organization leaders from different sectors of the economy, health care, technology, telecommunications, fintech, payments and security:

aetna	https://www.aetna.com/index.html
Arbor Networks	http://it.arbornetworks.com/
AT&T	https://www.att.com/
Bank of America	https://www.bankofamerica.com/
CA Technologies	https://www.ca.com/us.html
Capital One	https://www.capitalone.com/
Cisco	https://www.cisco.com/
Citrix	https://www.citrix.com/
Cybereason	https://www.cybereason.com/
Discover	https://www.discover.com/
Equifax	https://www.equifax.com/personal/
Experian	https://www.experian.com/
Idemia	https://www.idemia.com/
Intel	https://www.intel.com/content/www/us/en/homepage.html
J. P. Morgan	https://www.jpmorgan.com/country/US/en/jpmorgan
Kabbage	https://www.kabbage.com/
Mastercard	https://www.mastercard.us/en-us.html
McAfee	https://www.mcafee.com/en-us/index.html
Mozilla	https://www.mozilla.org/en-US/
Onfido	https://onfido.com/gb/
Palo Alto Networks	https://www.paloaltonetworks.com/
PNC Bank	https://www.pnc.com/en/personal-banking.html
Quicken Loans	https://www.quickenloans.com/
Rapid7	https://www.rapid7.com/
Red Hat	https://www.redhat.com/en
Symantec	https://www.symantec.com/
Tenable	https://www.tenable.com/
US Bank	https://www.usbank.com/index.html
Visa	https://usa.visa.com/
Wells Fargo	https://www.wellsfargo.com/

Collaboration and Sharing

One of main objectives of the center is bringing together leading companies to help develop innovative ideas that improve security, privacy and convenience for the US population.

For each initiative, the center publishes reports, promotes its activities and educates consumers, businesses and government. In particular:

- Within the **Cybersecurity Coalition** it submits written comments, offers testimony at US congressional and regulatory hearings, draft legal and policy white papers, engages with policymakers and holds events;
- The **Better Identity Coalition** in July 2018 published a report that outlines a comprehensive policy agenda for improving the privacy and security of digital identity solutions; and
- Via its **Hardware Vulnerability Project**, the center surveys the partners involved in the patching process and offers recommendations.

Multidisciplinary approach to cybersecurity

Center for Cybersecurity Policy and Law members include a wide variety of stakeholders, including the heads of large companies from different sectors of the economy, such as health care, technology, telecommunications, fintech, payments, and security.

This heterogeneous group of experts allows to the center to do the following while taking into account different points of view:

- Promote a vibrant and robust cybersecurity ecosystem;
- Support the development and adoption of cybersecurity innovations; and
- Encourage organizations of all sizes to take steps to improve their cybersecurity.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 11 Center for Cybersecurity Policy and Law Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	The center carries out a series of initiatives and projects focused on a range of critical cybersecurity issues.
Network of trust	It avoids negative behavior, takes on its own responsibilities, builds respected partnership and is reliable and trustworthy.
Collaboration and sharing	The Center for Cybersecurity Policy and Law organizes events and shares white papers and reports in order to stimulate cybersecurity dialogue and collaboration outcomes.
Multidisciplinary approach to cybersecurity	The group's list of members includes large companies and associations belonging to different industries and areas.

3.3.7 European Cyber Security Organisation – ECSO

Executive Summary

This case study examines the *European Cyber Security Organisation (ECSO)*, a fully self-financed nonprofit organization under Belgian law established in June 2016. It represents the industry-led contractual counterpart to the European Commission for the implementation of the cybersecurity contractual Public-Private Partnership (cPPP).

ECSO members include a wide variety of stakeholders such as large companies, SMEs, startups, research centers, universities, end-users, operators, clusters and association. It also counts on members from local, regional and national administrations from European Member States as well as countries that are part of the European Economic Area (EEA), the European Free Trade Association (EFTA) and H2020 associated countries.

This case study is based on desk research of reports related to the organization's cyber initiative.

European Cyber Security Organisation Initiative

ECSO's [47] main objective is to support all types of initiatives or projects that aim to develop, promote and encourage European cybersecurity. It focuses in particular on the following:

- Foster the growth of the European Digital Single Market and protect it from cyber threats;
- Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry with an increased market position; and
- Develop and implement cybersecurity solutions for the critical steps of trusted supply chains in sectoral applications where Europe is a leader.

ECSO is engaged in taking concrete actions to achieve these objectives:

- Collaborate with the European Commission and national public administrations to promote Research and Innovation (R&I) in cybersecurity;
- Propose a Strategic Research and Innovation Agenda (SRIA) and a multiannual roadmap with its regular updates;
- Foster market development and investments in demonstration projects and pilots to facilitate bringing innovation to the cybersecurity market;
- Foster competitiveness and growth of the cybersecurity industry in Europe (large companies and SME) as well as end users/operators through innovative cybersecurity technologies, applications, services and solutions;
- Support the widest and best market uptake of innovative cybersecurity technologies and services for professional and private use;
- Promote and assist in the definition and implementation of a European cybersecurity industrial policy to encourage the use of cybersecurity solutions as well as secure and trustworthy ICT solutions to increase digital autonomy; and
- Support the development and the interests of the entire cybersecurity and ICT security ecosystem (including education, training awareness, etc.).

Impact

ECSO members are organized into working groups and task forces in order to tackle the following priority issues, as defined by the ECSO board of directors:

Standardization, certification, labeling and supply chain management

This working group addresses the following issues:

- The EU ICT security certification framework. ECSO liaises with the European Commission and contributes to the European ICT security certification framework proposal which was published in 2017;
- Standards for interoperability;
- EU cybersecurity labelling;
- Increased digital autonomy; and
- Testing and validation of the supply and value chain in Europe.

The working group is segmented into sub-working groups and is closely collaborating with other ECSO working groups, the European Commission, ENISA and European standardization bodies such as CEN/CENELEC and ETSI.

Market deployment, investments and international collaboration

This working group's mission can be summarized as follows:

- Develop and maintain a view on the cybersecurity industry in Europe as a whole as well as support ECSO members to improve their market knowledge (products and suppliers, but also cybersecurity insurance solutions);
- Design and facilitate innovative private and public investment capabilities to understand the dynamics of the market and create a community of investors, brokers and supporting industries;
- Support international trade establishing dialogue with main trade partners (US, China, Brazil and Japan) and initializing dialogue with developing countries.

Additionally, this working group is segmented into sub-working groups that focus on international cooperation, investments, innovative business models and market knowledge.

Sectoral demand

This WG allows ECSO to bring together cybersecurity stakeholders from various sectors in order to:

- Contribute to a set of industrial policy activities such as defining the needs of sectors for standardization/certification, education, training and exercises and local/regional impact;
- Support the widest and best market uptake of innovative cybersecurity technologies and services by accelerating the wide diffusion of cybersecurity technologies in different industry sectors and creating new business opportunities;
- Support the use of innovative and trusted cybersecurity solutions and services for major societal and economic challenges in Europe, e.g. in different essential services providers, particularly in areas where Europe has a

competitive advantage. These areas include health, energy, transport, internal security, public services/eGovernment, ICT mobile and fixed devices/networks, Industry 4.0;

- Improve risk management with better metrics;
- Improve digital trust and facilitate information exchange;
- Develop the EU ICT security market and employment;
- Demonstrate the use of innovative cybersecurity solutions in the different verticals; and
- Understand user needs and available solutions/services/technologies from suppliers for different verticals.

Support to SMEs, coordination with countries (in particular East and Central EU) and regions

This WG focuses on the following issues:

- Support the development of SMEs, startups and high growth companies;
- Develop coordinated activities between clusters (both business oriented and triple helix), regions and local bodies (for local implementation of solutions/educations);
- Development of East and Central EU public and private sectors dealing with cybersecurity.

The working group is segmented into sub-working groups and is closely collaborating with Interreg Europe CYBER [48], a five year project aiming to boost the competitiveness of European cybersecurity SMEs and to create synergies among the EU cybersecurity valleys.

Education, awareness, training, cyber ranges

This WG focuses on the following issues:

- Increase education and skills on cybersecurity products and safe use of IT tools in Member States for individual citizens and professionals;
- Cybersecurity training and exercise ecosystem leveraging upon cyber range environments; and
- Awareness raising and basic hygiene skills.

The working group is segmented into sub-working groups and collaborates with Europol's European Cybercrime Centre (EC3) [49] and the National High Tech Crime Unit of the Netherlands' police [50] for the 'No More Ransom' campaign that aims to assist victims in the recovery of their encrypted files without paying a ransom, provide advice and raise awareness of the problem of ransomware in the public arena.

SRIA and Cyber Security Technologies

This WG focuses on the following objectives:

- Coordination of results and expectations from European Commission and R&I projects;
- Coordination of cybersecurity activities across cPPPs and EU initiatives;
- Support of cPPP implementation and H2020 cybersecurity projects; and
- Detailed suggestions for the 2017-2020 European Commission Work Program using an updated and focused SRIA.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote and encourage European cybersecurity, including:

- Promoting Research and Innovation (R&I) in cybersecurity;
- Proposing a Strategic Research and Innovation Agenda (SRIA) and a multiannual roadmap with its regular updates; and
- Fostering demonstration projects and pilots to facilitate bringing innovation to cybersecurity market.

Each working group is focused on a particular subpart of ECSO 's strategy. The results are published by means of reports and presented during organized events [51], such as the one organized together with EIT Digital to support cybersecurity scaleups and SMEs.

Governance

ECSO is a membership-based organization that gives each of its members a unique opportunity to actively shape the future of cybersecurity strategic research and innovation and build a sustainable market in Europe.

Potential members should be:

- Legal entities established in an ECSO country (EU Member State or an EEA/EFTA country or an H2020 associated country); or
- A public body from an ECSO country.

Categories of members:

- **Large companies:** These entities develop and/or manufacture cybersecurity solutions or provide services;
- **National and European organizations/associations:** These organizations represent their members' interests at the national or European level. They also represent their organizations on an international level;
- **SMEs:** Associations composed only by SMEs, startups, incubators and accelerators;
- **Users/operators of national public administrations or private companies (large or SMEs):** These organizations are directly represented;
- **Regional and local public administrations:** Regional/Local Clusters of public/private Legal Entities with local economic/ecosystem development interests;
- **Public administrations at a national level:** These organizations are directly represented;
- **Research centers, academia and universities:** Associations composed only by Research centers, academia or universities; and
- **Others:** These include financing bodies, insurances, consultants, etc.

The following diagram lays out how ECSO is organization and the interaction that exists between the existing different departments.

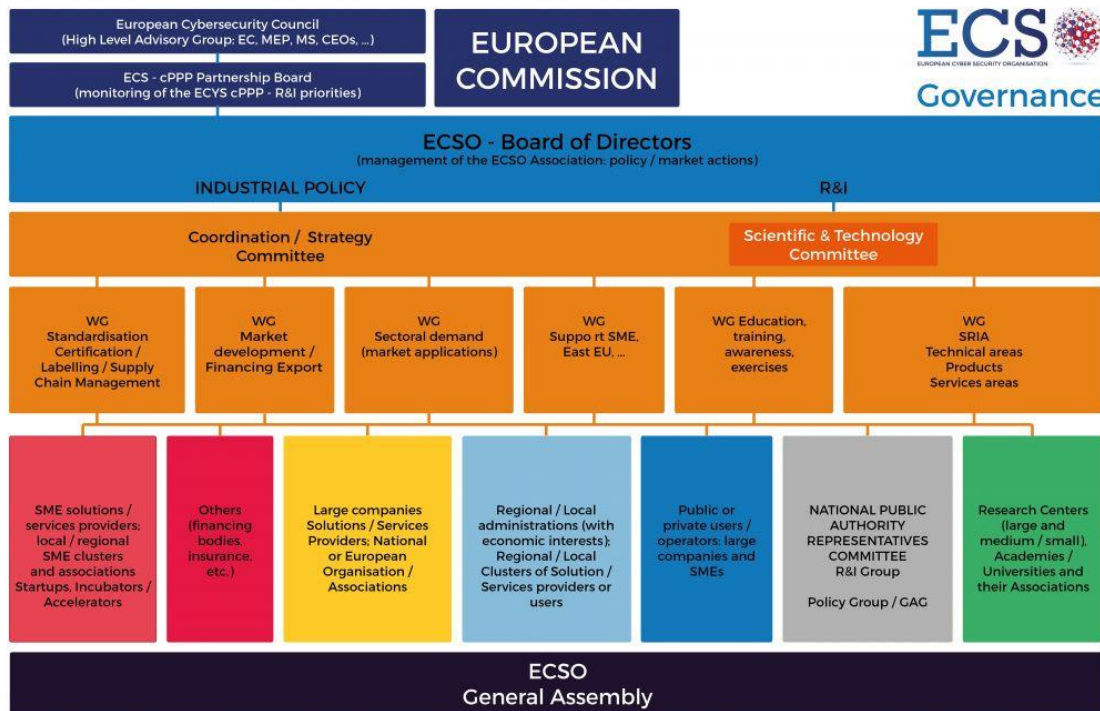


Figure 5 ECSO organization

All the activities are carried out based on ECSO Board of Directors directives. This Board is made up of large companies, SMEs, associations, users and operators, public administrations, RTO and universities, regions and clusters that work together in order to achieve initiative objectives.

ECSO key areas of activity

ECSO's main areas of interest can be summarized in seven main thematic priority areas:

- European ecosystem for cybersecurity that includes:
 - Cyber Range and simulation;
 - Education and training;
 - Certification and standardization; and
 - Dedicated support to SMEs.
- Demonstrations for society, economy, industry and vital services on following areas:
 - Industry 4.0 (Industrial Control Systems);
 - Energy (Smart Grids);
 - Smart Buildings & Smart Cities;
 - Transportation (including Automotive/Electrical Vehicles);
 - Healthcare; and
 - E-services for public sector, finance and telecommunications.
- Collaborative intelligence to manage cyber threats and risks:
 - GRC: Security Assessment and Risk Management;
 - PROTECT: High-assurance prevention and protection;

- DETECT: Information Sharing, security analytics and cyber threat detection; and
- RESPONSE and RECOVERY: Cyber threat management, response and recovery.
- Remove trust barriers for data-driven applications and services:
 - Data security and privacy;
 - ID and distributed trust management (including DLT); and
 - User centric security and privacy.
- Maintain a secure and trusted infrastructure in the long-term:
 - ICT protection; and
 - Quantum resistant crypto.
- Intelligent approaches to eliminate security vulnerabilities in systems, services and applications:
 - Trusted supply chain for resilient systems; and
 - Security and privacy by-design.
- From security components to security services

Multidisciplinary approach to cybersecurity

ECISO members include a wide variety of stakeholders such as large companies, SMEs, startups, research centers, universities, end-users, operators, clusters and association. Members also include government representatives at the local, regional and national level from European Member States as well countries that are part of the European Economic Area (EEA), the European Free Trade Association (EFTA) and H2020 associated countries.

The full list of ECISO members, categorized as mentioned above, can be consulted in [52].

Case Study Analysis Results

The case study results are summarized in the following table:

Table 12 European Cyber Security Organization Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	ECISO has a document of intent that outlines the strategy and the purpose of the initiative.
Governance	The organization has nominated a board to monitor, provide advice, track activities and gain community support.
ECISO key areas of activity	ECISO has defined a value generation initiative plan.
Multidisciplinary approach to cybersecurity	The organization has involved stakeholders in large companies, SMEs, startups, research centers, universities, end-users, operators, clusters and association. It also includes government representations on a local, regional and national level from European Member States as well as countries that are part of the European Economic Area (EEA), the European Free Trade Association (EFTA) and H2020 associated countries.

3.3.8 European Union Agency for Network and Information Security – ENISA

Executive Summary

The **European Union Agency for Network and Information Security (ENISA)** [53] is a center of expertise for cybersecurity in Europe. The agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens.

It is studied because of its active contribution to the high level of **network and information security (NIS)** within the European Union and the development of a culture of NIS in society. Furthermore, ENISA itself is a good example of cooperation between Member States, European Union bodies and relevant NIS stakeholders, including the private sector and on international level. Additionally, it is active in the area of education and awareness of NIS skills.

This case study is based on desk research of cyber initiative reports and semi-structured interviews with key leaders in this initiative.

ENISA's Cyber Initiative

The mission of European Network and Information Security Agency (ENISA) is to contribute to securing Europe's information society by raising "awareness of network and information security and developing and promoting a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations."

ENISA works closely together with the Member States of the European Union and the private sector to deliver advice and solutions. This includes the pan-European cybersecurity exercises, the development of national cybersecurity strategies, CSIRT cooperation and capacity building. ENISA also publishes reports and studies on cybersecurity issues. It has produced studies on:

- Cloud security;
- Data protection;
- Privacy enhancing technology & ensuring privacy for new technologies;
- Electronic identification and electronic trust services; and
- Identifying cyber threats.

ENISA provides practical advice and solutions for the public and private sectors in EU countries and for the EU institutions [54]. This includes:

- Organizing cross-Europe cyber crisis exercises;
- Assisting in the development of national cybersecurity strategies; and
- Promoting cooperation between computer emergency response teams and capacity building.

Additionally, ENISA helps draft EU policy and law on network and information security. This also contributes to economic growth in Europe's internal market.

The main focus of ENISA's activities to achieve its objectives are:

- Collate, analyze and make information and expertise available on key NIS issues that could potentially impact the EU, taking into account the evolutions of the digital environment;

- Assist and advise European Union institutions and Member States in developing and implementing EU policies, guidance and law on all matters relating to NIS;
- Assist Member States and European Union institutions on reinforcing their NIS capacities;
- Enhance cooperation at an EU level among Member States, European Union bodies and relevant NIS stakeholders, including the private sector; and
- Improve the management of its resources and engage more efficiently with its stakeholders, including Member States and Union institutions, as well as at an international level.

Impact

The mid-term ENISA priorities for the next 3 years are the following [55]:

- Anticipate and support Europe in facing emerging network and information security challenges;
- Promote network and information security as an EU policy priority;
- Support Europe in maintaining state-of-the-art network and information security capacities;
- Foster the emerging European network and information security community; and
- Reinforce ENISA's impact, by improving the management of its resources and engaging more efficiently with its stakeholders.

In addition, ENISA, following the technological trends and needs of the community, is invested in supporting the private and public sector in understanding the security benefits and drawbacks of Cloud Computing and Big Data. In this regards ENISA has written a number of papers on Cloud Computing Security and recently focused on Big Data security.

For more than ten years, ENISA has been supporting the cooperation between CSIRTs and the development of the CSIRT network. This network has become a good practice example in itself when it comes to cooperation between its members. ENISA's work on cooperation between CSIRTs and other operational communities is at the heart of a pan-European collaboration network of CSIRTs.

Recent deliberate disruptions of critical automation systems prove that cyber attacks have a significant impact on critical infrastructures and services. Disruption of these ICT capabilities may have disastrous consequences for EU Member States governments and social wellbeing. The need to ensure ICT robustness against cyber attacks is thus a key challenge at national and pan-European level.

In this regard, ENISA is also active in the area of education and awareness, using its knowledge to promote NIS skills. ENISA is also supporting and organizing cyber exercises. Cybersecurity training material was introduced in 2008. ENISA supports the development of ICT security standards and certification frameworks in Europe.

ENISA is also working on the line of technology for privacy in the online and mobile world. Moreover, it analyzes and proposes security measures for the protection of personal data, following a risk-based approach. Particular emphasis has been given to cryptographic protocols and tools and their possible implementation in real-life applications. The agency studies possible mechanisms for online and mobile data

protection, including transparency and control tools, accountability mechanisms, data erasure and portability techniques.

Moreover, in a constantly changing cyber threats environment, EU Member States need to have flexible and dynamic cybersecurity strategies to meet new and global threats. A national cybersecurity strategy (NCSS) is a plan of action designed to improve the security and resilience of national infrastructures and services. It is a high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. Currently, all countries in the European Union have a National Cyber Security Strategy (NCSS) as a key policy feature, helping them to tackle risks which have the potential to undermine the achievement of economic and social benefits from cyberspace.

Apart from tackling cybersecurity risks, ENISA's strategy builds on collaboration. Some of the most important ENISA's efforts to improve collaboration between stakeholders include information sharing and the creation of Public-Private Partnerships.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

ENISA's strategic objectives are derived from the ENISA regulation, inputs from Member States and relevant communities, including the private sector;

Good reputation

ENISA is the European Union Agency for Network and Information Security (NIS), established in 2004. As set out in 2013 in its renewed mandate, ENISA has been set up for the purpose of contributing to a high level of Network and Information Security within the Union contributing to growth and employment in Europe.

ENISA key areas of activity

ENISA's activities are focused in three areas:

- Recommendations;
- Activities that support policy making and implementation; and
- "Hands on" work, in which ENISA collaborates directly with operational teams throughout the EU.

Tracking progress, evaluate and adjust strategy

Reports presenting the findings and conclusions from the external evaluation of ENISA's core operational activities are provided with the objective of providing ENISA with an evaluation of its performance and an assessment of the possible options for change and improvement.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 13 ENISA Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	ENISA 's objectives are clearly defined by regulation, inputs from Member States and relevant communities.
Good reputation	There is a high level of Network and Information Security within the European Union, which contributes to growth and employment in Europe.
3 key areas of activity	<ul style="list-style-type: none"> o Recommendations; o Policy making and implementation; and o "Hands On" work
Tracking progress, evaluate and adjust strategy	There are reports on that evaluate ENISA 's performance and an assessment of the possible options for change and improvement.

3.3.9 EIT Digital

Executive Summary

This case study examines *EIT Digital*, a leading European digital innovation and entrepreneurial education organization driving Europe's digital transformation. It is focused on entrepreneurship and is at the forefront of integrating education, research and business by bringing together students, researchers, engineers, business developers and entrepreneurs.

This is done at its pan-European network of co-location centers in Berlin, Eindhoven, Helsinki, London, Paris, Stockholm, Trento, Budapest and Madrid. The organization also has a hub in Silicon Valley that aims to create a true two-way bridge between the European ecosystem of EIT Digital and the Bay Area ecosystem.

This case study is based on desk research on Action Lines [56], the EIT Digital Challenge [57] and the EIT Digital Accelerator [58].

EIT Digital Initiative

EIT Digital [59] is a leading European open innovation organization that invests human and financial resources in key high potential activities for the development of ICT business and talent in Europe.

The investments are clustered in a total of eight pan-European Innovation and Education Action Lines - portfolios of thematic activities targeting impactful outcomes. Action Lines are executed within a European ecosystem of top corporations, SMEs, universities, research institutes and startups, and in co-location centers.

The Innovation Action Lines have been strategically chosen and are as follows:

- **Digital Industry** that covers the seamless process from production to retail and the related supporting functions such as logistics and consumer engagement;
- **Digital Cities** that leverages the digital transformation of the cities through centralized, participative and collaborative interactions between city actors, including

- government, city service providers, industry, and citizens;
- **Digital Wellbeing** that aims to slow down the growth of healthcare expenses and maintain the quality of life during the working life and at higher age;
- **Digital Infrastructure** that is the core enabler of the digital transformation by providing secure, robust, responsive and intelligent communications and computation facilities; and
- **Digital Finance** that since 2018 supports the creation of innovative tools and services to help the finance industry adapt to the challenges it currently faces.

In each Action Line, EIT Digital has selected the most promising research results, disruptive technologies and business strategies from its ecosystem and beyond and has packaged them in innovation activities and startups. EIT Digital ambition is to drive these innovations to succeed in world markets and become European success stories.

The EIT Digital Academy Action Lines consists in:

- **EIT Digital Master School** that trains graduates pursuing digital entrepreneurial education;
- **EIT Digital Doctoral School** that provides the opportunity for industry embedded, market focused doctorates; and
- **EIT Digital Professional School** that ensures those already working within industry are able to keep abreast of current developments and use them to help their organization innovate and succeed.

All the above mentioned Action Lines (both Innovation and Education) are executed within EIT Digital European ecosystem of top corporations, SMEs, startups, universities and research institutes and localized in its "nodes" in Berlin, Budapest, Eindhoven, London, Madrid, Helsinki, Paris, Stockholm, Trento and its hub in Silicon Valley.

Each node operates a physical "co-location center" where most of the activities are carried out. EIT Digital bring together professionals, ideas, technologies and investments in these spaces that turn the co-location centers into vibrant hot spots where students, researchers, engineers and business developers interact to succeed in the market.

The goal of EIT Digital's Silicon Valley Hub is to create a true two-way bridge between the European ecosystem of EIT Digital and the Bay Area ecosystem by:

- Strengthening the European ecosystem;
- Coordinating hub actions with the European partners that already have connections to the Bay Area; and
- Collaborating with the local consulates of European countries.

Impact

EIT Digital invests in strategic areas to accelerate the market uptake of research-based digital technologies focusing on Innovation Action Lines. Each Action Line is a portfolio of activities. On one hand, there are open innovation activities carried out by partners. Meanwhile, on the other hand, there are fast-growing technology startups that are ready to scale commercially. These entrepreneurial projects are grounded in game-changing research results, high-profile technologies and disruptive business strategies.

Within Digital Industry Action Line, EIT Digital has an initiative called the **Operate European Digital Industry with Products and Services (OEDIPUS)**. OEDIPUS is a high impact initiative that pursues the creation of digital industry innovation hubs. These hubs would act as hot spots of the digital transformation of the manufacturing industry and would represent a unique opportunity to create products and services for a "smart industry." In particular, it would create an opportunity to explore the combination of Open Platforms with proprietary Industry Cloud and Enterprise Systems and understand which new business models this combination could generate and support.

In the Digital Cities Action Line, mobility, information and safety are the anchor points for innovations taken into consideration. A multidisciplinary approach including service design, urbanism, and social sciences is used to provide an accurate understanding of the concrete problems cities are facing and the means to overcome these, in particular by developing sustainable business models.

The Digital Wellbeing Action Line leverages digital technologies to stay healthy (prevention and early detection) or cope with an existing chronic condition. The solutions rely on enabling consumers to be well-informed about their wellbeing and to be able to use digital instrumentation to monitor and improve their quality of life.

A key aspect of the Digital Infrastructure Action Line is to catalyze cooperation across the networking, computing and security domains.

Within this Action Line, the high impact initiative **Advanced Connectivity Platform for Vertical Segments (ACTIV8)** addresses the Internet of Things market, which currently is in its early stages and dominated by domain-specific platforms. The platform is made up of proprietary architectures and vertically divided technology silos, providing a unified approach for developers and industry to support the widespread growth of the Internet of Things.

ACTIV8 has active collaboration with and between the leading European companies, universities, research institutes, and startup, such as Aalto University, Bittium/SafeMove, Engineering, Ericsson, KTH Royal Institute of Technology, Politecnico di Milano, RISE SICS and Tampere University of Technology.

The Digital Finance Action Line focuses on the three most important aspects for the finance industry:

- **The future of retail banking**

focused on future interaction between financial institutions and retail customers and providing a broad range of themes including cybersecurity, authentication, online payments, micropayments,

cashless societies and personal financial management;

- **Modernized corporate banking**
promoting tools that help to create better financial transparency, automate and simplify financial and accounting tasks for companies, ensure fluid and secure lending, and improve financial services available to corporates, SMEs and startups in Europe; and
- **Digitalized wealth/asset management**
supporting technologies like machine learning and artificial intelligence algorithms to provide better advice, structure better financial products, improve reporting and support investment professionals in selecting the best financial products to withstand systemic risks.

Based on above mentioned Action Lines, EIT Digital organizes the EIT Digital Challenge, a contest focused on fast-growing European deep tech scaleups. The startups must be in late stages and be actively seeking to accelerate their growth [60]. In 2018, 25 finalists were selected for each category to pitch their product or service in front of an international jury of corporations and investors.

The two best companies per category gain 12 months in the EIT Digital Accelerator (international business growth services) worth €50,000 to scale up their business internationally. On top of that, the first prize winner in each category receives a cash prize of €50,000.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

The main purpose of EIT Digital is to invest human and financial resources in key high potential activities for the development of ICT business and talent in Europe. EIT Digital focuses on incubation, market uptake and rapid growth of these innovations.

As such, EIT Digital focuses its investments on a limited number of innovation areas that have been selected with respect to European relevance and leadership potential. The Innovation Action Lines are as follows:

- **Digital Industry;**
- **Digital Cities;**
- **Digital Wellbeing;**
- **Digital Infrastructure;** and
- **Digital Finance.**

Once the activities are selected, the EIT Digital Accelerator steps in to fully manage the innovation and entrepreneurship funnel, supporting the growth of the activities so that they become successful European products, services or ventures.

In addition to coaching the business, the accelerator helps them with pan-European Access-to-Market (customer acquisition) and Access-to-Finance (fundraising).

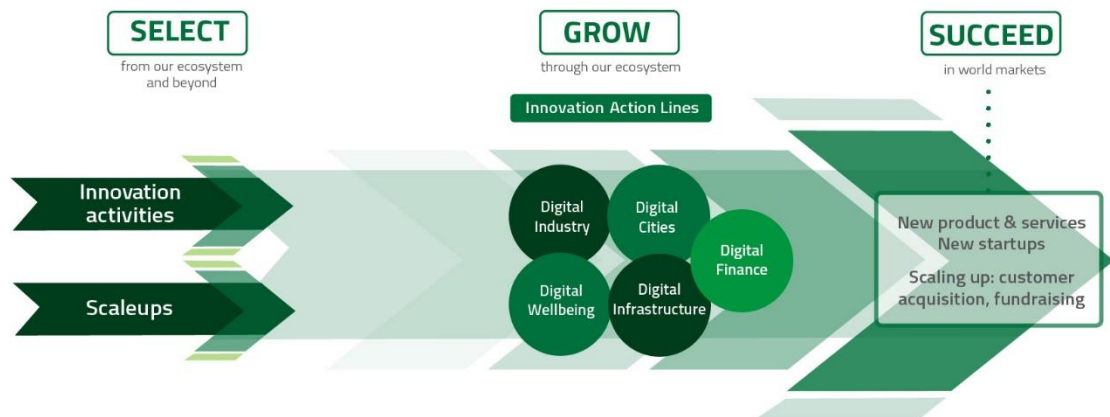


Figure 6 EIT Digital Strategy

Good reputation

Since 2012, the EIT Digital Accelerator has supported over 270 startups, allowing them to access new markets and gain funding partly because of their connection to an organization a good reputation.

The results and impact of EIT Digital are at the heart of the priorities recently identified by the European Commission and national governments.

In the recently published proposal for the 2021-2027 EU budget there is an increased investment in digital through a strong EIT Digital in Horizon Europe (overall increased focus on Digital) and an additional €9 billion for the Digital Europe program. Several EU Member States have announced increased investments in digital technology, notably in artificial intelligence and cybersecurity.

Successful execution of those plans requires talented professionals, skills, technology and new business ideas. Since its launch on 2012, EIT Digital has:

- Equipped more than 1,500 students with the skills to innovate and become entrepreneurs;
- Supported more than 270 startups and scaleups and helped them grow internationally;
- Created 60 new companies as a result of innovation activities; and
- Launched more than 250 products and services commercially.

EIT Digital continues to build on these strong achievements and welcomes the increased investment in digital skills and technology at the EU and Member State level. This strong mandate allows EIT Digital to have global impact through European innovation fueled by entrepreneurial talent and digital technology.

EIT Digital key areas of activity

As already stated, EIT Digital focus its investments on a limited number of innovation areas called Innovation Action Lines:

- **Digital Industry;**
- **Digital Cities;**

- **Digital Wellbeing;**
- **Digital Infrastructure;** and
- **Digital Finance.**

The **Digital Industry Action Line** covers the seamless process from production to retail and the related supporting functions such as logistics and consumer engagement. The mission of the Action Line is to improve efficiency in production and retail, to better address customer needs and to help save natural resources in manufacturing and logistics. Within this value chain, a large amount of data and knowledge is produced and shared. This data has an increasing share of the value in the entire business domain.

The **Digital Cities Action Line** leverages the digital transformation of cities through centralized, participative and collaborative interactions between city actors, such as government, city service providers, industry, and citizens. This transformation enables the deployment of disruptive information, mobility and safety services in the cities.

The **Digital Wellbeing Action Line** aims to slow down the growth of healthcare expenses while maintaining quality of life during for workers and senior citizens by providing prevention and coping services for mental and physical conditions. Aging, working longer and living longer unfortunately do not imply that there are also more healthy work and living years. The result is a strong increase in occupational and individual healthcare costs.

The **Digital Infrastructure Action Line** is the core enabler of the digital transformation. It provides secure, robust, responsive and intelligent communications and computation facilities.

More specifically, it targets:

<i><u>Networking:</u></i>	the mobile broadband infrastructure, network softwarization, and the Internet of Things; and
<i><u>Computing:</u></i>	Cloud Computing, Big Data and Artificial Intelligence; and
<i><u>Security:</u></i>	privacy, cybersecurity and digital ID management.

EIT Digital set up the **Digital Finance Action Line** in 2018 to support the creation of innovative tools and services to help the finance industry adapt to the challenges it currently faces. Robust yet agile and tailored financial services are essential for our economies, citizens and enterprises.

Multidisciplinary approach to cybersecurity

A key aspect of the Digital Infrastructure Action Line (one of the five EIT Digital action line) is to catalyze cooperation across the networking, computing and security domains. This creates added value by deeply integrating technologies that typically are only very loosely coupled. Distributed cloud solutions that are secure and privacy aware for real-time processing based on close integration of networking, computing and security will support new industry segments that are latency sensitive, such as automotive industry or process industry segments.

In September 2018, together with the European Cybersecurity Organization (ECISO) [61], EIT Digital organized the third edition of the ECISO event “**#InvestCyber STRATEGIC BUSINESS MATCHMAKINGS.**”

The event aimed to support European scaleups and SMEs by providing them with a unique opportunity to showcase their technology and to introduce themselves to industry leaders looking for the most promising cybersecurity solutions.

The event comprised a special training by an EIT Digital dedicated team of experts for the 25 selected scaleups, which has prepared them to be ready for the “Pitch Session” with potential customers.

Moreover, EIT Digital has been directly involved in the **Security Tools for App Development (STAnD)** project, a new plug-in that helps application programming interface (API) developers make their APIs secure by providing a managed security service capable of identifying potential vulnerabilities together with a catalogue of code hardening techniques that help reduce their exploitation.

STAnD is the outcome of EIT Digital’s new API Assistant Innovation Activity. Its commercial launch is scheduled at the end of 2018 in Italy. In 2019, it will be launched in Spain and Germany.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 14 EIT Digital Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	EIT Digital invests human and financial resources in key high-potential activities for the development of ICT business and talent in Europe.
Good reputation	The organization has supported more than 270 startups. The results and impact are aligned with European Commission priorities.
EIT Digital key areas of activity	EIT Digital focuses investments on a limited number of innovation areas.
Multidisciplinary approach to cybersecurity	Finally, the organization catalyzes cooperation across the networking, computing and security domains by integrating technologies that typically are only very loosely coupled.

3.3.10 Mind the Bridge – MTB

Executive Summary

Mind the Bridge (MTB) [62] is a global organization that provides innovation advisory services for corporates and startups. Based in Silicon Valley with offices in San Francisco, London, Italy and Spain, MTB has been working since 2007 as an international bridge at the intersection between startups and corporations. MTB was established in 2007 by the then Googler, Marco Marinucci.

It is studied because of its active contribution and successful example of fostering a sustainable and global entrepreneurial ecosystem. Their programs and activities focus on bringing startups and corporates together to enhance the growth of all parties and to bring new value to enterprises through innovation.

This case study is based on desk research of MTB's cyber initiative reports and semi structured interview with key leaders involved in these efforts.

MTB's Cyber Initiative

MTB believes there is societal value in embracing the principles of entrepreneurship as a key accelerator of economies. Their goal is to foster a sustainable and global entrepreneurial ecosystem. MTB programs and activities focus on bringing startups and corporations together to enhance the growth of all parties and to bring new value to enterprises through innovation.

MTB's focus on startups include initiatives such as:

- Startup school;
- Matching events;
- Mind the Seed – established to invest in seed stage companies; and
- Startup Europe Partnership (SEP) - the integrated pan-European open innovation platform that helps the best EU scale-ups grow.

MTB's focus on corporations include initiatives such as:

- Supporting corporate open innovation;
- Technology scouting – scouting for corporations and dedicated matching programs; and
- Advisory services to corporations include licensing, investments, due diligence and acquisitions.

They publish curated reports [63] on the status of the startup economy in different geographies, M&A and innovation market trends in various verticals. They enjoy strong partnerships with entities such as the London Stock Exchange, Euronext and the European Commission. MTB runs the Commission's Start-up Europe Partnership open innovation platform.

Additionally, Mind the Bridge has been running a non-profit foundation since 2007. It was established by Marco Marinucci with the support of a group of entrepreneurs passionate about entrepreneurship education.

MTB organizes the following regular events:

- **SEC2SV** - Launched in 2015, Startup Europe Comes to Silicon Valley (SEC2SV) is an annual event that brings together the most relevant founders, corporates, investors and policymakers from the EU entrepreneurial ecosystem and Silicon Valley in engaging meetings and workshops. The event helps create meaningful long-term relationships.
- **SEC2IL** - Startup Europe Comes to Israel (SEC2IL) aims at bringing together corporations, investors, entrepreneurs, and policymakers from the EU entrepreneurial ecosystem and Israel each year.
- **SEP 2.0** - Startup Europe Partnership (SEP) focuses on offering an integrated pan-European platform to help the best startups emerge from these local ecosystems and scale-up.

Impact

MTB has established a startup school. This is part of their education program that immerses founders in a startup ecosystem for up to 3 weeks, giving them valuable experiences to take back to their home countries. The program consists of workshops, mentor sessions, corporate visits and pitching exercises. Unstructured networking time and local excursions are also included to help participants engage fully with the ecosystem.

Mind the Bridge also works to bring startups and corporations together during matching events, as well as in case-by-case scouting calls by corporates. Participation in these matching sessions allows startups to interact with the innovation departments of established corporations in their industry.

Mind the Seed [64] was established in 2008 by MTB founder Marco Marinucci to invest in seed stage companies. The organization is still active today and has a portfolio of over 30 deals. Mind the Seed occasionally takes interest in companies that attend Mind the Bridge startup school sessions. MTS invests in 8 to 12 startups per year, providing both seed funding and value-added services by engaging professionals with significant experience in startups, venture investment and the intricacy of the Silicon Valley ecosystem.

Startup Europe Partnership (SEP) is the integrated pan-European open innovation platform that helps the best EU scale-ups grow. The Start-up Europe Partnership is a platform where the best scale-ups meet the best corporations and investors with a single goal: make things happen. Whether that means procurement (product licensing or initiating co-development/POCs), investments and exits (acquisitions and IPOs). Start-up Europe Partnership (SEP) hosts "Europe's Corporate Start-up Stars," a ranking of the most start-up friendly corporations in Europe each year. SEP also connects the European ecosystems with Silicon Valley (SEC2SV mission) and Israel (SEC2IL mission).

Mind the Bridge provides a suite of advisory services to assist corporates in their open innovation processes. Their services enable their open innovation drive to be more efficient and more effective.

Mind the Bridge provides dedicated technology scouting services for medium to large size corporations in search of new technologies in their field and beyond. Their team is capable of filtering hundreds of startups from around the world in search of the right solutions to their client's needs.

Mind the Bridge has experience in scouting for industry leaders in multiple countries, and has kick started and connected many innovation departments with disruptive and cutting-edge startup technologies. MTB also plans and hosts dedicated matching boot camps for corporations looking to scout in a specific vertical. These intense 1-3 day sessions at Mind the Bridge in San Francisco expose corporations to a group of selected startups in their given vertical.

MTB is investigating innovation ecosystems. It regularly produces reports with the goal of sharing insights and data about startup ecosystems in order to give relevant parties a macro overview of the current landscape. Key areas of research are:

- **Startup M&A:** Annually produced in partnership with Crunchbase analysis and data about startup acquisitions worldwide.

- **Scale-ups:** As part of Startup Europe Partnership, MTB publishes a mix of continent-wide reports and country-specific reports (SEP Monitor), as well as reports on current trends in the scale-up landscape in Europe and the US.
- **Open Innovation:** MTB analyzes the current trends and scenarios in corporate startup collaboration, including a map of international companies having an innovation outpost in Silicon Valley; and
- **Policy:** SEP policy reports and briefs are aimed at providing data and recommendations to support policies (Digital Single Market and Scale-up of Start-up Ecosystems).

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

The goal of Mind the Bridge is to foster a sustainable entrepreneurial ecosystem, spur more innovative ideas and reinvigorate the new venture economy, providing a 360-degree entrepreneurship education.

Good reputation

Since 2007, Mind the Bridge has been working as an international bridge at the intersection between startups and corporations. It scouts, filters and works with 1500+ startups a year and supports global corporations in their innovation quest, driving open innovation initiatives that often translate in curated deals with startups.

Mind the Bridge key areas of activity

Mind the Bridge activities are focused on

- *Innovation Advisory services for Corporations* working on education, incentive programs, technology scouting and innovation advisory; and
- *Entrepreneurship programs for startups and scaleups* providing a startup school, bringing startups and corporations together during matching events, investing, organizing Startup Europe Comes to Silicon Valley (SEC2SV) and Startup Europe Partnership (SEP).

Mind the Bridge foundation.

Mind the Bridge has been running a nonprofit foundation since 2007. It was established by Marco Marinucci with the support of a group of entrepreneurs passionate about entrepreneurship education. In 2012, in order to invest in startups with an international soul, Marco Marinucci created a seed investment fund that invests in 6 to 12 startups per year providing both seed funding and value-added services.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 15 MTB Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	MTB's goal is to foster a sustainable entrepreneurial ecosystem, spur more innovative ideas and reinvigorate the new venture economy.
Good reputation	MTB has been working as an international bridge at the intersection between startups and corporations since 2007.
key areas of activity	<ul style="list-style-type: none"> o Innovation Advisory services for corporations o Entrepreneurship programs for startups and scaleups
MTB foundation	A nonprofit foundation of entrepreneurs passionate about entrepreneurship education.

3.3.11 Office of Compliance Inspections and Examinations – OCIE

Executive Summary

This case study examines the **Office of Compliance Inspections and Examinations (OCIE)**, which is part of SEC (US Securities and Exchange Commission). The Office of Compliance Inspections and Examinations administers the SEC's nationwide examination and inspection program for registered self-regulatory organizations, broker-dealers, transfer agents, clearing agencies, investment companies and investment advisers.

OCIE serves as the "eyes and ears" of the SEC. It conducts examinations of regulated entities to promote compliance, prevent fraud, identify risk and inform policy.

The office conducts inspections to foster compliance with the securities laws, detect violations of the law and to keep the SEC informed of developments in the regulated community. Among the more important goals of the examination program is the quick and informal correction of compliance problems. When the SEC finds deficiencies, it issues a "deficiency letter" identifying the problems that need to be rectified and monitors the situation until compliance is achieved. Violations that appear too serious for informal correction are referred to the Division of Enforcement.

OCIE is organized into several offices and program areas to best support and carry out the mission of the National Exam Program (NEP).

This case study is based on desk research that took into consideration OCIE web's page [65], the 2018 National Exam Program Examination Priorities [66], the Compliance Outreach Program [67] and the Offices and Program Areas.

Office of Compliance Inspections and Examinations Initiative

OCIE [68] conducts the SEC's National Exam Program (NEP). The NEP's mission is to protect investors, ensure market integrity and support responsible capital formation through risk-focused strategies that:

- Improve compliance;
- Prevent fraud;
- Identify and monitor risk; and
- Inform policy.

The results of the NEP's examinations are used by the SEC to inform rule-making initiatives, identify and monitor risks, improve industry practices and pursue misconduct.

NEP staff promote compliance with federal securities laws through exams, outreach, publications and, where appropriate, referrals to the SEC's Division of Enforcement.

OCIE work stands on the above mentioned four "pillars" and is organized into several offices and program areas to best support and carry out the mission of the National Exam Program (NEP):

- **The Investment Adviser/Investment Company (IA/IC) Examination Program.** The IA/IC examination program is responsible for conducting exams of investment advisers and investment companies, such as mutual funds and exchange-traded funds.
- **The Broker-Dealer and Exchange (BDX) Examination Program.** The BDX examination program is responsible for conducting exams of broker-dealers, national securities exchanges, transfer agents, municipal advisors, the Public Company Accounting Oversight Board and the Securities Investor Protection Corporation.
- **The Clearance and Settlement (CS) Examination Program.** The CS examination program is responsible for conducting exams of clearing agencies, some of which have been designated as systemically important financial market utilities.
- **The FINRA and Securities Industry Oversight (FSIO) Examination Program.** The FSIO examination program is responsible for conducting exams of the Financial Industry Regulatory Authority and the Municipal Securities Rulemaking Board.
- **The Technology Controls Program (TCP).** TCP is responsible for conducting examinations of entities subject to Regulation Systems Compliance and Integrity (SCI). This program area also administers the SEC's CyberWatch program, which is the primary intake point for information filed under Regulation SCI.
- **The Office of Risk and Strategy (ORS).** ORS conducts risk assessment, market surveillance, quantitative analysis, large firm monitoring and focuses on operational strategy in support of each of the program areas within the NEP.
- **The Office of Chief Counsel (OCC).** OCC provides advice on law, policy, operations and ethics to examiners across the NEP; coordinates with other regulators; reviews proposed legislation and rulemaking; and serves as a liaison for investigations and audits of OCIE.

OCIE is one of the cosponsors, along with the SEC's Division of Investment Management and the Division of Enforcement's Asset Management Unit ("AMU"), of **the Compliance Outreach Program** (formerly CCO outreach) **for investment companies and investment advisers.**

The mission of the Compliance Outreach Program is to improve compliance by opening the lines of communication between SEC staff and Chief Compliance Officers (CCOs) and other senior officers of registered investment advisers and investment companies.

The program is designed to provide a forum to discuss compliance issues in a practical way, to share experiences and to learn about effective compliance practices. The program features a number of elements, including regional events at various locations across the country and national events sponsored in Washington, DC.

OCIE, in coordination with the SEC Division of Trading and Markets, is a cosponsor, along with the Financial Industry Regulatory Authority ("FINRA"), of **the Compliance Outreach Program for Broker-Dealers**.

The 2017 National Compliance Outreach Program for Broker-Dealers is been a one-day program intended for compliance, audit and other senior personnel of broker-dealer firms and branch offices. The program provides an open forum for regulators and industry professionals to share strong compliance practices and promote the exchange of ideas to develop an effective compliance structure.

The program focuses on issues related to cybersecurity, senior investors and regulatory hot topics such as anti-money laundering and recidivist brokers. Additionally, senior leaders from the SEC and FINRA discuss the regulatory environment.

Impact

OCIE prime commitment is to protect retail investors, including seniors and those saving for retirement, with a close look at products and services offered to retail investors, as well as the disclosures they receive about those investments.

OCIE does this by conducting examinations targeting circumstances in which retail investors may have been harmed and reviewing whether financial service professionals have met their legal obligations.

Compliance with the securities laws overseen by the SEC has helped make US markets some of the safest and most vibrant in the world.

The SEC National Exam Program fosters compliance and helps fulfil the SEC's mission of protecting investors, maintaining fair, orderly and efficient markets and facilitating capital formation.

As of 2017, the population of registered entities that OCIE oversees consisted of more than 4,000 broker-dealers (including approximately 162,000 branch offices and 640,000 registered representatives), more than 12,000 investment advisers (with nearly \$67 trillion in assets under management), approximately 850 fund complexes (representing close to 11,000 mutual funds and exchange-traded funds) and more than 400 transfer agents and over 650 municipal advisors.

In addition, OCIE has oversight responsibility of 20 national securities exchanges, the Financial Industry Regulatory Authority (FINRA), the Municipal Securities Rulemaking Board (MSRB), the Securities Investor Protection Corporation (SIPC), eight clearing agencies and the Public Company Accounting Oversight Board (PCAOB). The Dodd-Frank Wall Street Reform and Consumer Protection Act increased OCIE's responsibilities to include security-based swap dealers, security-based swap data repositories, major security-based swap participants and securities-based swap execution facilities. Additionally, the Jumpstart Our Business Act expanded OCIE's responsibilities to include oversight of crowdfunding portals.

Publication of examination priorities is a valuable tool for the efforts to promote compliance and protect investors.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

OCIE publishes its **examination priorities** annually to improve compliance, prevent fraud, monitor risk and inform policy. In general, the priorities reflect certain practices, products and services that OCIE believes may present potentially heightened risk to investors and/or the integrity of the US capital markets.

Of particular interest for 2018 were matters involving critical market infrastructure, duties to retail investors and developments in cryptocurrency, initial coin offerings and secondary market trading.

In 2018, OCIE's examination priorities were broken down into five categories:

- Compliance and risks in critical market infrastructure;
- Matters of importance to retail investors, including seniors and those saving for retirement;
- FINRA and MSRB;
- Cybersecurity; and
- Anti-money laundering programs.

The collaborative effort to formulate the annual examination priorities starts with feedback from examination staff, who are uniquely positioned to identify the practices, products and services that may pose significant risk to investors or the financial markets. OCIE staff also seek advice of the SEC Chairman and Commissioners, staff from other SEC Divisions and Offices, the SEC's Investor Advocate and the SEC's fellow regulators.

Throughout the year OCIE adds priorities (beyond those published annually) as it identifies emerging risks and trends and responds to tips, complaints and referrals. OCIE regional offices also initiate exams based on their local assessment of risk and knowledge of their registrant population.

This publication has the objective to provide transparency into issues and areas that constitute, for OCIE, an appropriate focus for upcoming year and which entail the most effective use of examination resources in fulfilling OCIE mission.

Make a risk analysis

The sheer size and continued growth of the securities industry prevents OCIE from conducting regular comprehensive examinations of each registered firm. In order to effectively oversee all of the varying market participants within its jurisdiction, and given its limited resources, OCIE utilizes a **risk-based strategy**. A central part of this effort is ongoing analysis of root causes of harm to investors and markets and the identification of the greatest risks. The analysis flows into a number of aspects of its program, including process for setting priorities, the criteria it uses to select potential examination candidates and determining the appropriate scope of its exams, as well as resource allocation more generally.

Effort to be data-driven

Use of data is integral to the program and complements the risk-based exam approach and use of technology. Data are used in areas such as risk assessment and exam scoping, planning and execution.

There are rapid advancements in the capacity to use data to analyze regulatory filings and trading activity. Among other things, this has included development by Quantitative Analytics Unit (QAU) of the National Exam Analytics Tool (NEAT) to facilitate the analysis of trading blotters. The QAU is composed of financial engineers who, in addition to developing tools, directly assist exam teams with quantitative analysis. Data analytics, ever more sophisticated, is used to identify potential non-compliance with the securities laws, including possible fraudulent behavior. Data is also used to better identify high-risk exam candidates and to more efficiently analyze information during examinations. OCIE continuously looks for ways to employ technology and data analytics to enhance its effectiveness in every aspect of the examination program.

Transparency

Transparency is an important tool. Publicly sharing certain information about the examination program (particularly priorities, common findings and what is considered highest risk areas) will ultimately benefit investors by assisting the work of legal, compliance and risk staff at registered entities as they work within their organizations to achieve compliance with the securities laws. To this end, OCIE has been publishing more information about what is doing, why is doing it and what it has found and learned in the process.

Risk alerts, in particular, have become a valuable tool, and they are published more frequently. The ultimate goal of these Risk Alerts is to promote compliance.

Recent topics in Risk Alerts include the most frequently-cited deficiencies from various examination initiatives, as well as observations of industry practices and compliance issues from cybersecurity examinations. Sharing this information helps registered firms (particularly those that have not been examined recently) sharpen their identification and correction of deficient practices, maximizing the impact of the examination program and resulting in better protection for investors.

The NEP published six Risk Alerts to the industry in FY 2017 and four Risk Alerts in FY 2018 [69].

Collaboration and sharing

OCIE is a cosponsor of the Compliance Outreach Program for:

- Funds and advisers;
- Broker-dealers;
- Municipal advisers; and
- Entities subject to Regulation Systems Compliance and Integrity (SCI Entities).

It is designed to provide a forum to discuss compliance issues, share experiences and learn about effective compliance practices. The program includes, but varies according to target, events, roundtables and ways to facilitate interaction via communication (e.g. mail address to ask questions).

Tracking progress, evaluating and adjusting strategy

OCIE relies heavily on its talented and experienced staff, many of whom are subject matter experts in key risk areas. OCIE also increasingly leverages technology and data in its risk assessment and examination processes. OCIE continually assesses its resource deployment and asks: *"Are we using our resources in way that maximizes the benefit to investors?"*

In fiscal year 2017, the National Exam Program completed over 2,870 examinations (representing an 18 percent increase over FY 2016).

Key areas of activity

OCIE embraces innovation and new technology, both as a means to do more with less and as a necessary focal point of analytic efforts.

Technology in the financial markets often spurs innovation in ways that are beneficial to investors. It has the potential, for example, to help drive down costs for investors and provide new ways for people to access financial markets, investment information and financial advice. Where technological advances lead to new business models, OCIE seeks to assess their potential impact on the financial markets, identifies ways investors may be harmed, if any, and works with colleagues to share critical observations that may assist the SEC in adapting to emerging risks and concerns.

OCIE also seeks to keep pace with advancing technology, to monitor for cybersecurity risks, to engage with industry in efforts to help combat cybersecurity attacks and to prevent investor harms.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 16 Office of Compliance Inspections and Examinations Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	OCIE publishes examination priorities annually to improve compliance, prevent fraud, monitor risk and inform policy.
Make a risk analysis	The organization identifies the greatest risks and defines a risk plan.
Effort to be data-driven	OCIE uses data for risk assessment, exam scoping, planning and execution.
Transparency	It publishes information about examination programs and Risk Alerts.
Collaboration and sharing	OCIE co-sponsors programs and organizations events and communication efforts.
Tracking progress, evaluate and adjust strategy	The organization continually assesses resource deployment and utilization of technology and data in risk assessment and examination processes.
Key areas of activity	It uses innovation and new technology for the benefit of the market and investors. OCIE also embraces these tools to monitor cybersecurity risks, to help combat cybersecurity attacks and to prevent investor harms.

3.3.12 United States Coast Guard – USCG

Executive Summary

This case study examines the **United States Coast Guard (USCG)**, the principal US federal agency responsible for maritime safety, security and environmental stewardship in the nation's ports and waterways. In this capacity, the Coast Guard protects and defends more than 100,000 miles of US coastline and inland waterways and safeguards an Exclusive Economic Zone (EEZ). This encompasses 4.5 million square miles stretching from North of the Arctic Circle to South of the equator, from Puerto Rico to Guam, covering nine time zones (the largest EEZ in the world).

As one of the five Armed Services of the United States, the Coast Guard is the only military branch within the Department of Homeland Security. In addition to its role as an Armed Service, the Coast Guard is a first responder and humanitarian service that provides aid to people in distress or those impacted by natural and man-made disasters whether at sea or ashore. The Coast Guard is a member of the US Intelligence Community and is a law enforcement and regulatory agency with broad legal authorities associated with maritime transportation, hazardous materials shipping, bridge administration, oil spill response, pilotage and vessel construction and operation.

This case study is based on desk research and analysis of the USCG's webpage [70], mission [71], cyber strategy [72] and initiatives to improve cybersecurity [73].

United States Coast Guard Initiative

The Coast Guard carries out three basic roles, which are further subdivided into eleven statutory missions. The three roles are:

- Maritime safety;
- Maritime security; and
- Maritime stewardship.

The eleven statutory missions as defined by US law are divided into homeland security missions and non-homeland security missions.

The overall mission of the US Coast Guard is to ensure the safety, security and stewardship of US waters. In the digital age, however, there is no strategic objective the Coast Guard can adequately meet or operational mission the Coast Guard can fully perform without a robust and comprehensive cyber program.

Cyber technology is linked with all aspects of Coast Guard mission performance. It simultaneously presents opportunities for greater efficiency and effectiveness in the operating environment, while fueling new threats and challenges.

In 2015, the USCG introduced the US Coast Guard's Cyber Strategy to guide its efforts in the cyber domain. This strategy identifies three distinct strategic priorities that are critical to overall mission success:

- Defending Cyberspace;
- Enabling Operations; and
- Protecting Infrastructure.

This strategy provides a framework for the Coast Guard's efforts in the cyber domain over the next ten years, which will be essential to ensure US security and prosperity in the maritime environment. This framework will enable success across all Coast Guard mission areas and will support all aspects of the "Prevent-Respond" core operational concept.

The Coast Guard must adapt to the ongoing and rapid advancements in cyber technology. In continuing its history of responding to the ever-evolving maritime needs of the US, the Coast Guard will fully embrace cyberspace as an operating domain.

Impact

Government systems, including Coast Guard systems, face a mounting array of emerging cyber threats that could severely compromise and limit the service's ability to perform its essential missions.

Adversaries employ sophisticated tools and possess substantial resources. They include state-sponsored and independent hacker groups, terrorists and Transnational Organized Crime groups as well as corrupt, disgruntled and complacent employees (commonly referred to as insider threats).

These growing threats also pose significant risks to the US Maritime Transportation System (MTS) and critical infrastructure. By direct extension, this is a threat to US security and economic stability.

With approximately 360 sea and river ports, which handle more than \$1.3 trillion in annual cargo, the US is critically dependent on a safe, secure and efficient MTS, which in turn is highly dependent on a complex, globally-networked system of automated cyber technology. With over 90% of the nation's goods moving via increasingly networked maritime conveyance, preserving cybersecurity is essential to overall safety, security and effectiveness.

Best Practices

The following good practices have been identified based on an analysis of the case. These best practices may possibly be key factors in enabling collaboration between different parties that belong to different backgrounds, cultures and environments.

Clear purpose and strategy

The Coast Guard is committed to ensure the safety, security and stewardship of US waters. This commitment requires a comprehensive cyber strategy that provides a clear framework for overall mission success.

USCG Cyber strategy focuses on:

- Defending Cyberspace;
- Enabling Operations; and
- Protecting Infrastructure.

To achieve these goals, USCG has established or is considering cyber-focused initiatives [73], which will also improve the US's cyber protection and response ability.

The **Coast Guard Strategic Plan 2018-2022 [74]** (that serves as a strategic framework), among multiple strategic priorities and objectives, reports these specific priorities for cybersecurity:

- *Strategic priority 1, Objective 1.2* **MODERNIZE - ASSETS, INFRASTRUCTURE AND MISSION PLATFORMS.** This includes the modernization of the Cyber and Intelligence (C5I) enterprise with the objective to strengthen the reliability of C5I Enterprise Systems.
- *Strategic priority 2, Objective 2.2* **ENHANCE - UNIFIED EFFORT.** This includes enhanced partnerships with maritime stakeholders to share universal best practices with the aim to strengthen maritime cybersecurity preparedness, response and recovery to safeguard the MTS.

Cybersecurity and defense interoperability

An owner or operator of a vessel or facility that is required to maintain an approved security plan must report activities that may result in a transportation security incident to the National Response Center (NRC), including breaches of security and suspicious activity.

The US Coast Guard handles all reports of security incidents as Sensitive Security Information (SSI), in accordance with 49 CFR part 1520, which includes requirements for proper marking and storage. The information is therefore not subject to routine public disclosure. The US Coast Guard will share the information with other law enforcement agencies on a need to know basis. [75]

Make a risk analysis

Development of industry segment-specific profiles (*Cybersecurity Framework Profiles*) was led by the USCG's Office of Port and Facility Compliance (CG-FAC), along with the National Institute of Standards and Technology and the National Cybersecurity Center of Excellence. These profiles are risk assessment tools tailored to specific maritime industry segments. The profiles present a minimum state of cybersecurity and cyber risk management and provide the opportunity to plan for future business decisions.

These risk assessment profiles were created for the Maritime Bulk Liquids Transfer, Offshore Operations and Passenger Vessel Operations segments. A fourth profile focused on Navigation and Automated Systems for Vessels and Facilities is now being developed.

Collaboration and sharing

Cyber risk management on vessels is promoted using an international approach. The US delegation worked with European Member States and industry representatives to develop the IMO (International Maritime Organization) MSC/FAL (Maritime Safety Center/Facilitation Committee) Circular Guidelines [76] for Maritime Cyber Risk Management and MSC Resolution 428(98) Maritime Cyber Risk Management in Safety Management Systems.

Marine Transportation System Cyber Awareness Training provides basic cyber awareness with a focus on maritime facility and vessel operations. The awareness training provides personnel basic knowledge of cyber terms and systems that may be encountered throughout the MTS.

Governance

The **Office of Cyberspace Forces** aims to implement the US Coast Guard Cyber Strategy and manage the cyber program. It delivers programmatic oversight and direction for the organization, training, equipping and operational policy for the cyberspace workforce and develops strategy and policy for enabling operations and protecting MTS infrastructure.

Multidisciplinary approach to cybersecurity

Enhancing Cybersecurity (2018) [77] Cyber threats are endemic to the government, public and private sector alike. In addition to protecting its own networks and systems, the Coast Guard actively assesses the cyber vulnerabilities that might hamper US maritime transportation system. By leveraging its authorities and promoting private-public partnerships, the Coast Guard works with industry to develop and implement measures that will secure critical maritime infrastructure from those who seek to do harm.

Good reputation

Enhancing Cybersecurity (2019) [78]. Virtually every aspect of modern life is undeniably linked to global networks and increasingly complex, frequent and malicious cyber activities pose serious threats to security and privacy. Guided by the tenets of its cyber strategy, the Coast Guard continues to invest in its own cybersecurity while developing a diverse cyber workforce to address this growing national security challenge. Leveraging 227 years of operational experience and relationships with state, local, tribal and territorial governments, as well as maritime industry partners, the Coast Guard is the trusted, physical presence in US ports and waterways.

By leveraging Captain of the Port authorities and 43 Area Maritime Security Committees, the Coast Guard works with federal, state, local, tribal and private sector stakeholders to develop measures, which promote cyber risk management to secure its critical maritime infrastructure from those who seek to do it harm.

Case Study Analysis Results

The case study results are summarized in the following table:

Table 17 United States Coast Guard Case Study Analysis Results

Practice/Activity	Evidence/Outcomes
Clear purpose and strategy	The USCG focuses on defending cyberspace, enabling operations and protecting infrastructure. It also publishes a strategic plan (that serves as a strategic framework).
Cybersecurity and defense interoperability	USCG asks the owner or operator of a vessel or facility to report activities that may result in a transportation security incident to the National Response Center (NRC), including breaches of security and suspicious activity.
Make a risk analysis	It develops industry segment-specific profiles that serve as risk assessment tools tailored to specific maritime industry segments.
Collaboration and sharing	The organization works with EU Member States and industry representatives to develop the IMO MSC/FAC Circular Guidelines for Maritime Cyber Risk Management and MSC Resolution 428(98) Maritime

Practice/Activity	Evidence/Outcomes
	Cyber Risk Management in Safety Management Systems. Marine Transportation System Cyber Awareness Training provides stakeholders with basic cyber awareness with a focus on maritime facility and vessel operations.
Governance	The Office of Cyberspace Forces implements the US Coast Guard Cyber Strategy and manages the cyber program.
Multidisciplinary approach to cybersecurity	The USCG works with the industry to develop and implement measures that will secure critical maritime infrastructure from those who seek to do harm.
Good reputation	With its operational experience and relationships with federal, state, local, tribal, and territorial governments, as well as maritime industry partners, the Coast Guard is the trusted, physical presence in US ports and waterways.

3.4 BEST PRACTICES

This section summarizes all the best practices identified in each case study and organizes them into a table. Based on the enhancement of the methodology introduced in this deliverable, the table reports the matching of the obtained list of best practices with the case studies in order to verify those applicable in each of them.

In following table, we highlight the best practice - case study association found during desk research phase with blue checkmark (✓) and the ones identified with D3.4 added methodology steps with green checkmark (✓). See Section 2 for more details.

We have identified the application of the best practices to the case studies based on explicit declarations found in the analyzed documentation. This doesn't mean that further associations cannot be considered for other case studies.

Table 18 Case Study Best Practices Table

Case Studies Best Practices													
		W & F Hewlett Foundation	DARPA	EU-NATO agreement	cPPP	Global EPIC	Center for Cybersecurity	ECOSO	ENISA	EIT Digital	Mind the Bridge	OCIE	USCG
Clear purpose and strategy	Definition of a clear purpose and identification of an accurate strategy for achieving it	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Coherence of intents	In a cooperation initiative, the strategies of all the stakeholders involved have to be coherent in order to easily achieve the intended objectives.		✓	✓	✓	✓	✓	✓	✓	✓	✓		
Foundation	Creation of a grant program in order to support and invest in initiative activities.	✓	✓		✓					✓	✓		
Sense of mission	Creation of a sense of mission in order to inspire people involved in the initiative.	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
Multidisciplinary approach to cybersecurity	Involvement of a heterogeneous group of experts in the activities related to cybersecurity and promoted and supported by the initiative.	✓	✓		✓	✓	✓	✓	✓	✓			✓
Countering hybrid threats	Involvement of a heterogeneous group of experts in the activities promoted and supported by the initiative.	✓		✓	✓	✓	✓	✓	✓				
Make a risk analysis	Inclusion of the risks in the strategy of the initiative.	✓									✓	✓	✓
Risk-taking and tolerance of failure	Inclusion of the risks and of tolerance of failure in the strategy of the initiative.		✓								✓		
Resilience key areas of activity	Definition of initiative key areas of activity in order to evaluate the resilience against attacks and anticipate emerging issues.	✓		✓	✓	✓			✓	✓		✓	✓
Governance	Definition of an initiative organization that monitors, advises and supports the community and stakeholders.	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Tracking progress, evaluating and adjusting strategy	Definition of metrics in order to track progress, assess the results achieved and adjustment of the strategy if necessary to reach the target. Execution of tests and exercises in order to check protocols defined and sharing of the results.	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Case Studies Best Practices													
		W & F Hewlett Foundation	DARPA	EU-NATO agreement	cPPP	Global EPIC	Center for Cybersecurity	ECOSO	ENISA	EIT Digital	Mind the Bridge	OCIE	USCG
Collaboration and sharing	Organization of public consultations in order to obtain feedback and suggestions from the stakeholders and share information.		✓		✓	✓	✓	✓			✓	✓	✓
Cybersecurity and defense interoperability	Definition of procedures in order to allow interaction and information sharing between cybersecurity and defense.		✓	✓									✓
Build effective communication pathways	Definition of a clear communication process in order to let stakeholders cooperate properly.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Foster cooperation	Cooperation, fostering and exchange of expertise in order to build partners' capacity and resilience.	✓	✓	✓	✓	✓			✓	✓	✓		✓
Strengthening political dialogue	Organization of regular meetings in order to strengthen political dialogue among countries involved in the initiative.		✓	✓	✓		✓		✓		✓	✓	✓
Good reputation	Acting in a way that allows the initiative or organization be attractive and build a good reputation within communities and with funders. This helps promote activities.	✓	✓	✓				✓	✓	✓	✓		✓
Transparency	Publish the activity reports in a public domain that can be consulted.	✓	✓		✓	✓	✓	✓	✓	✓		✓	
Network of trust	Involvement of organizations with good reputations within the initiative in order to easily obtain community trust during the initial phase.	✓	✓			✓	✓	✓	✓	✓			✓
Limited tenure and urgency	Definition of an organization mechanism that fosters new ideas and the passion for those ideas.		✓		✓	✓		✓		✓	✓		
Vibrant ecosystem	Establishment of a heterogeneous ecosystem of innovation.		✓		✓	✓	✓	✓		✓	✓		
Innovation key areas of activity	Definition of initiative key areas of activity in order to focus on a determined number of innovation areas and achieve better results.			✓	✓	✓		✓		✓	✓	✓	✓

Case Studies Best Practices													
		W & F Hewlett Foundation	DARPA	EU-NATO agreement	cPPP	Global EPIC	Center for Cybersecurity	ECSSO	ENISA	EIT Digital	Mind the Bridge	OCIE	USCG
Effort to be data driven	Use data in order to enhance the initiative’s strategy and carry out a risk analysis.		✔					✔	✔	✔	✔	✔	✔

3.5 GUIDELINES FOR INNOVATION PARTNERSHIP IN CYBERSECURITY AND PRIVACY

This section reports the results of our investigation applying the methodology described in Section 2. We identified as metrics the outcomes of the analysis of the initiatives and their impact. Additionally, we selected common approaches that represent good practices in order to enable mutually beneficial partnerships between different organizations from the EU and the US. These common approaches are shown in following table.

Table 19 Best Practices Category

Best Practices Tableau	
Have a strategy consistent with criteria	Clear purpose and strategy
	Coherence of intentions
	Foundation
	Sense of mission
Multidisciplinary approach to cybersecurity	Multidisciplinary approach to cybersecurity
Resilience	Countering hybrid threats
	Make a risk analysis
	Risk-taking and tolerance of failure
	Key areas of activity
	Effort to be data driven
Governance	Governance
	Tracking progress, evaluating and adjusting strategy
Cooperation and sharing	Collaboration and sharing
	Cybersecurity and defense interoperability

Best Practices Tableau	
	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

The Case Studies Table, shown in Table 20, summarize the common identified practices and indicates the case studies where each practice is more evident and documented.

In this table we highlight the common practice - case study association found using methodology introduced with D3.2 with a blue checkmark (✓) and the ones identified with D3.4 added methodology steps (see Section 2) with green checkmark (✓).

Table 20 Case Studies Table

Case Studies Tableau												
	W & F Hewlett Foundation	DARPA	EU-NATO agreement	cPPP	Global EPIC	Center for Cybersecurity	ECSSO	ENISA	EIT Digital	Mind the Bridge	OCIE	USCG
Have a strategy to be consistent with certain criteria	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multidisciplinary approach to cybersecurity	✓	✓		✓	✓	✓	✓	✓	✓			✓
Resilience	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Governance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cooperation and sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reputation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Innovation		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓

The next sections illustrate each practice and why it has been selected as a good one for enabling innovation partnership between EU and US.

3.5.1 Have a strategy to be consistent with certain criteria

Any entity, regardless of the sector it belongs to (whether it is a research institute, a private company or a public authority), needs to outline its aims and the initiatives it intends to carry out to achieve them.

In many cases, drafting an official definition of intent, disseminating a strategic document and describing a list of activities with a plan of implementation characterizes the scope of work and makes the interests accessible and clear to the community.

Having a precise strategy and laying out how implement it to achieve the stated goals reassures the members of a community so that they can compare their goals with the strategy of the organization and assess whether, on the basis of common or compatible objectives, a partnership can be advantageous.

Once the strategy has been defined, be consistent with it and pursue what was planned. In addition, it is important to provide contributions to demonstrate what has been done. This helps to increase an organization's reliability and build a good reputation.

Some examples:

- The **Hewlett Foundation** clearly outlines the purpose of its cyber initiative and identifies an accurate strategy for achieving it. The foundation launched the cyber initiative in March 2014 and refined its goals and strategy in an updated document in 2016. The official foundation website dedicates a section to the "Cyber" which is very clear and schematic, describing its goals, ideas and practices are described. Additionally, the foundation's grant making is fully reported. Some articles and a "Learn more" section provide in-depth information about cyber initiatives.
- In the **EU-NATO agreement**, the document specifies the objectives to be pursued by the parties under which the agreement has been signed.
- The **Global EPIC** initiative was launched in October 2017 during the 3rd European Cybersecurity Forum – CYBERSEC 2017 in Krakow, Poland. The website of the ecosystem summarizes the initiatives. Meanwhile, the terms of reference document describes, in a concise and clear way, the purpose and the background of the initiative. It includes the values, partners and the organization of the community.
- The **cPPP** was implemented in 2016 and remains in force until December 2020. The acts of the agreements are public. The cPPP objectives are clear and well described. The parties involved in the agreement have specific responsibilities and duties.
- The main objective of **ECISO** is to support all types of initiatives or projects that aim to develop, promote and encourage European cybersecurity.
- Strategic objectives of **ENISA** are derived from the ENISA regulation and inputs from the EU Member States and relevant communities, including the private sector.

- **EIT Digital** focuses its investments on a limited number of innovation areas that have been selected with respect to European relevance and leadership potential.
- **Mind the Bridge** has the goal to foster a sustainable entrepreneurial ecosystem, spur more innovative ideas and reinvigorate the new venture economy, providing a 360-degree entrepreneurship education.
- **OCIE** publishes its examination priorities annually to improve compliance, prevent fraud, monitor risk and inform policy. Throughout the year OCIE adds priorities (beyond those published annually) as it identifies emerging risks and trends and responds to tips, complaints and referrals.
- **USCG** focuses on defending cyberspace, enabling operations and protecting infrastructure. It periodically publishes a Strategic Plan (that serves as a strategic framework).

3.5.2 *Multidisciplinary approach to cybersecurity*

Cybersecurity involves all aspects of people's lives, even those that are not directly related to information technology or computer science. Organizations belonging to the most disparate areas are facing issues related to the security of data and the protection against malicious attacks.

A multidisciplinary approach to cybersecurity has become essential to address these issues. More and more partnerships and consortia between organizations that deal with different areas are created in order to build a common front to face the challenges of cybersecurity and privacy. The goal is to bring each one's own skills and their own points of view and from this sharing generate new business, align demand to supply, anticipate future problems.

Some examples:

- The **cPPP** involves the EC and a large list of entities, including large companies, SMEs and associations belonging to different industries and areas.
- Experts from education, policy, industry, government, think tank, academia and civil society are involved in achieving the **Hewlett Foundation** objectives.
- **DARPA** is fueled by partners in multiple sectors (university, industry, small business, government, public and media).
- Education, policy debate, experts from industry, government, think tank, academia and civil society are involved in achieving the **Global EPIC** objectives.
- **ECISO** members include a wide variety of stakeholders, such as large companies, SMEs, startups, research centers, universities, end-users, operators, clusters and associations.
- One of the five **EIT Digital** Action Lines (Digital Infrastructure) focuses on catalyzing cooperation across the networking, computing and security domains, integrating technologies that typically are only very loosely coupled.
- By leveraging its authority and promoting private-public partnerships, the **US Coast Guard** works with the industry to develop and implement

measures that will secure critical maritime infrastructure from those who seek to do harm.

In an international context, specifically for partnerships between organizations in the EU and the US, a multidisciplinary approach is an even greater added value because it provides a broader vision. Additionally, it considers different geo-political and cultural backgrounds.

3.5.3 Resilience

Nowadays, we are witnessing the birth of many organizations or even startups that often have a short life and do not regret adapting to the dynamism of the market. Establishing partnerships with weak companies can cause damage to an organization. It is comparable to a wrong investment which can generate a loss money, time and resources.

Resilience is defined as "*the capacity to recover quickly from difficulties*" [6] and it is an enabler for cooperation and partnerships. For an organization, it is important to be ready to face unexpected or damaging events that could harm it. It must have a risk plan or some risk prevention measures in order to guarantee its survival.

Some examples:

- The **EU-NATO agreement** aims to boost the ability to counter **hybrid threats** by bolstering resilience, working together on analysis, prevention, and early detection. This is done through timely information sharing and, to the extent possible, intelligence sharing between staffs.
- The **Hewlett Foundation** included the risks in their strategy paper. The foundation considers the risks from the definition of its own strategy and keeps the risk document updated.
- Openness to new ideas, risk-taking and tolerance of failure are essential elements of **DARPA** innovation. Proposals submitted to DARPA are reviewed by government experts with advice on specific topics from subject-matter experts both within and outside the government. The Source Selection Board makes recommendations to help the agency decide whether or not to invest.
- Ecosystems within **Global EPIC** want to share knowledge and experience, contribute to a structured discussion on how to evaluate the resilience of system-of-systems against cyber attacks, enable horizon scanning, anticipation of emerging issues, analyze trends and investigate theories of new domains.
- **ECSO** is focused on seven main thematic priority areas.
- **ENISA's** activities are focused in three areas: recommendations, activities that support policy making and implementation and "hands on" work. In the last area, ENISA collaborates directly with operational teams throughout the EU.
- **OCIE** utilizes a risk-based strategy. The central part of the strategy is the ongoing analysis of root causes of harm to investors and markets and the identification of the greatest risks. The use of data is integral to the program and complements the risk-based exam approach and the utilization of technology.

- **USCG** develops industry segment-specific profiles that serve as risk assessment tools tailored to specific maritime industry segments.

3.5.4 Governance

Governance is related to a set of principles, rules and procedures concerning the management and the supervising of an organization. It is intended to increase the accountability of an organization while also declaring its ethical principles, which are essential in the establishment of a partnership. Organizations which share ethical and moral principles can share also business objectives. In addition, providing details about the organization of activities and practical information about processes and procedures will facilitate collaboration. It can be considered an enabler for the industry for engagement in cybersecurity and privacy R&I projects.

Processes and rules can diverge between EU and US organizations because of they refer to different geo-political, legal, cultural and historical contexts. Thus, governance could be not suitable for some organization given its background. Knowing the processes of governance of an organization or community could be an enabler for joining or for addressing issues when establishing the partnership.

Some examples:

- The **cPPP** has established a board for monitoring, advising, community support. It is the official communication channel between the European Commission and the ECSO Association to discuss the Horizon 2020 Cybersecurity cPPP Work Program activities.
- In the **Hewlett Foundation**, indicators of progress are identified. For example, increased amounts of specified outputs, like research, collaborations and funding. Leveraging an outside evaluator to assess the efforts, the Hewlett Foundation can adjust its strategy in real-time as needed.
- The **EU-NATO agreement** has step up coordination on exercises, including on hybrid, by developing as the first step parallel and coordinated exercises for 2017 and 2018.
- **DARPA** has a rigorous approval process for deciding which projects to fund. Agency leadership must agree to support a program before millions or tens of millions of dollars are committed to it.
- **Global EPIC** describes in detail the government process it will follow, emphasizing the equality of members in rights and duties, the alternation in the decision-making board and also providing practical information about the meeting organization to facilitate interaction and to improve the work of the community members.
- All the activities are scheduled based on the directives from the **ECSO** Board of Directors. This board is made up of large companies, SMEs, associations, users and operators, public administrations, RTOs, universities, regions and clusters that work together in order to achieve initiative objectives.
- **ENISA** provides reports on the evaluation of its performance and an assessment of the possible options for change/improvement.
- **OCIE** continuously assesses resource deployment and utilization of technology and data in risk assessment and examination processes.
- **USCG**, with the Office of Cyberspace Forces, implements its cyber strategy and manages the cyber program.

3.5.5 Cooperation and sharing

Cooperation and information sharing are fundamental to face the new challenges in cybersecurity and privacy. Nowadays, organizations are increasingly convinced of the importance of putting together one's own experiences, skills and data since it is becoming essential to have a winning approach. The analysis of the case studies we considered for our investigation has demonstrated the growing need to create multi-disciplinary communities in which each organization brings its own point of view and its own resources to reach a common goal.

It is clear that addressing cybersecurity and privacy issues is no longer the prerogative of experts in a specific sector. All sectors can benefit from and take advantage of cooperation.

This is an even more determining factor if we think about building partnerships between Europe and the United States. Although each jurisdiction is subject to different regulations and has a different culture and history, they certainly share points of interest and have common goals. Collaboration allows for a comparison analysis to take place and foments debate, which provides possibilities for improvements.

Some examples:

- **Global EPIC** involves entities that are committed to combining their knowledge, experience and expertise to achieve common goals. The organization's ecosystems bring together academia, industry and government to respond to cybersecurity threats and enable economic development opportunities. Global EPIC's 14 ecosystems have largely developed independently, driven by local and national objectives. The leaders of these initiatives have become aware that the challenges of cybersecurity require global paradigm-shifting partnerships and cooperation that reflect regional and local imperatives. Underpinning this perspective is a conscious attempt to 'glocalize' – localize the global and globalize the local.
- The **cPPP** initiative was created with the intent of enabling collaboration between the private and public sector. Cooperation and sharing is one of the key points of the agreements. Public consultations are periodically organized in order to obtain feedback and suggestions from the stakeholders. This feedback is used to stimulate cybersecurity dialogue and collaboration outcomes.
- The **EU-NATO agreement** is a virtuous example of organizations that share competencies and resources for mutual benefits. A stronger NATO and a stronger EU are mutually reinforcing, and deep cooperation between the two organizations is necessary in order to develop new ways of working together and create new levels of ambition.
- **OCIE** is a cosponsor of Compliance Outreach Programs designed to provide a forum to discuss compliance issues, to share experiences and to learn about effective compliance practices.
- The **USCG** asks the owners or operators of a vessel or facility to report activities that may result in a transportation security incident to the National Response Center (NRC), including security breaches and suspicious activity. USCG will share, if needed, the information with other law enforcement agencies (not public disclosure). USCG also delivers awareness training to provide personnel with a basic knowledge of cyber terms and systems. It

works with EU Member States and industry representatives to develop guidelines.

3.5.6 Reputation

An organization's reputation is essential to its survival. 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 this modern age of social networking, websites and other methods of instant communication, organizations must be conscientious of their reputations on a constant basis and be responsive to any crisis that may have an impact on their reputation.

While it is an intangible concept, having a good reputation can benefit an initiative in many ways, including: community and organization preference; support for an organization in times of crisis or controversy; and the future value of an organization in the marketplace.

Before the age of social media sites such as Twitter, LinkedIn or Facebook, the reputation of an organization was tied to word-of-mouth promotion, publications, meetings and event attendance and careful public relations. Maintaining the reputation of an organization through social media takes time and requires educating stakeholders within the organization, making them aware of an initiative's internal values and key messages that need to be conveyed as well as creating a united, consistent voice.

Some examples:

- The **Hewlett Foundation** leverages its experience, the quality of grantees, ongoing investments and strategic communication to build a good reputation.
- **Global EPIC** is a new initiative, but the 14 co-founders have a consolidated experience in the cybersecurity environment.
- **ENISA** is the European Union Agency for Network and Information Security (NIS), established in 2004. ENISA has been set up for the purpose of contributing to a high level of Network and Information Security within the European Union contributing to growth and employment in Europe.
- Since 2012, the **EIT Digital** Accelerator has supported over 270 startups and helped them gain access new markets and gain funding. This has been done by providing startups with a link to an organization with a good reputation.
- Since 2007, **Mind the Bridge** has been working as an international bridge at the intersection between startups and corporations.
- **OCIE** has been publishing more information about what it is doing, why is doing it and what it has found and learned in the process.
- Leveraging 227 years of operational experience and relationships with state, local, tribal and territorial governments, as well as maritime industry partners, the **USCG** is the trusted, physical presence in US ports and waterways.

3.5.7 Innovation

Innovation is essential for the growth of any company and organization. The secret to the success of innovative organizations is associated with their ability to get the best out of the creative minds of their employees. This requires an innovative culture where everyone is able to think independently.

Research on innovation spans many fields of inquiry, including business, economics, engineering and public administration. Studies of innovation in organizations investigate what external and internal conditions induce innovation, how organizations manage the innovation process and in what ways innovation changes organizational conduct and outcomes.

Today, in the social media era, crowdsourcing and open innovation are two ways to allow people to work together on a massive scale for innovation. In this way, an organization can benefit from an idea, wisdom and creativity from the outside. Nonetheless, it could be difficult to manage a large-scale project and maintain a working relationship with crowdsourced workers.

Some examples:

- **DARPA** has a vibrant ecosystem of innovation. The agency operates and is fueled by partners in multiple sectors (university, industry, small business, government, public and media).
- Matchmaking between ecosystem entities as well as the generation of a global framework program for research and innovation are fundamental factors for the success of **Global EPIC**.
- **EIT Digital** focuses its investments on a limited number of innovation areas (Innovation Action Lines).
- **Mind the Bridge** activities are focused on innovation advisory services for corporations as well as on entrepreneurship programs for startups and scaleups.
- **OCIE** embraces innovation and new technology, both as a means to do more with less and as a necessary focal point of analytic efforts.

4 CONCLUSIONS

In this document, twelve case studies were selected based on their relevance to innovation in cybersecurity and privacy topics. The consortium also considered some partnerships already in place between the EU and the US as success stories, which provides virtuous examples of good practices for enabling collaboration. A case study methodology has been applied. For each case study, a deep analysis on their main aspects has been conducted. A qualitative approach for gathering the case study methodology result has been chosen.

The study has highlighted some common practices that can be considered good practices – some of them are derived from current existing partnerships between organizations belonging to the geographical areas the project focuses on – for enabling or enhancing partnerships between the EU and the US. These good practices can also be used to stimulate industry engagement in cybersecurity and privacy R&I projects.

The consortium produced this document for those who want to start an initiative, startups and innovator managers. It is AEGIS' hope that these successful best practices can help key stakeholders interested in EU-US cooperation jump start their efforts and provide them a roadmap to success.

5 REFERENCES

- [1] D 3.2 Guidelines for Innovation Partnership in cybersecurity and privacy V1 - v1.0.pdf
- [2] <https://www.ub-cooperation.eu/pdf/casestudyreport.pdf>
- [3] <http://www.gpmfirst.com/books/designs-methods-and-practices-research-project-management/practical-research-method-netlipse#ref913>
- [4] https://www.gao.gov/special.pubs/10_1_9.pdf
- [5] https://www.hewlett.org/wp-content/uploads/2016/09/Cyber-Initiative-Refined-Grantmaking-Strategy_2016.pdf
- [6] <https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp>
- [7] <https://en.oxforddictionaries.com/definition/resilience>
- [8] <https://www.hewlett.org/wp-content/uploads/2017/06/RTI-report-on-understanding-demand-for-cyber-policy-resources.pdf>
- [9] <https://www.hewlett.org/library/cyber-initiative-refined-grantmaking-strategy/>
- [10] <https://www.hewlett.org/>
- [11] <http://www.berkeley.edu/>
- [12] <http://web.mit.edu/>
- [13] <https://www.stanford.edu/>
- [14] <https://www.nyu.edu/>
- [15] <https://www.taxpayer.net/>
- [16] <https://carnegieendowment.org/>
- [17] <https://www.hewlett.org/grants/>
- [18] <https://www.hewlett.org/wp-content/uploads/2017/06/2016-DCA-report.pdf>
- [19] <https://www.hewlett.org/wp-content/uploads/2017/06/RTI-report-on-understanding-demand-for-cyber-policy-resources.pdf>
- [20] <https://www.hewlett.org/strategy/cyber/>
- [21] <https://www.darpa.mil/our-research?ppl=collapse&tFilter=15>
- [22] <https://www.darpa.mil/about-us/about-darpa>
- [23] http://www.dtic.mil/descriptivesum/Y2017/DARPA/DARPA_0400D_RD_TE_MasterJustificationBook_Defence_Advanced_Research_Project.pdf
- [24] <https://www.darpa.mil/program/cyber-grand-challenge>
- [25] https://www.darpa.mil/attachments/DARPA_Innovation_2016.pdf
- [26] <https://www.darpa.mil/program/cyber-grand-challenge>
- [27] [http://europa.eu/rapid/press-release MEMO-13-1159_en.htm](http://europa.eu/rapid/press-release_MEMO-13-1159_en.htm)
- [28] <https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp>
- [29] <http://www.apre.it/eventi/2018/i-semester/sc7-giornata-nazionale>

- [30] <https://www.ecs-org.eu/activities>
- [31] <https://www.leadersinsecurity.org/projects/cima-lsec-european-cyber-security-industry-market-analysis.html>
- [32] <http://www.ecs-org.eu/documents/uploads/wg4-position-paper.pdf>
- [33] <http://www.ecs-org.eu/documents/ecs-cppp-sria.pdf>
- [34] <http://www.bdva.eu/>
- [35] <http://www.effra.eu/>
- [36] <https://5g-ppp.eu/>
- [37] <http://www.ecs-org.eu/documents/uploads/membership-form.pdf>
- [38] <https://www.globalepic.org/ece/terms.php>
- [39] <https://www.globalepic.org/ece/index.php#>
- [40] <https://2017.cybersecforum.eu/global-cybersecurity-initiative-launched-strengthen-collaboration-between-regional-ecosystems/>
- [41] <https://www.globalepic.org/ece/joinus.php>
- [42] <https://centerforcybersecuritypolicy.org/>
- [43] <https://www.cybersecuritycoalition.org/>
- [44] <https://www.betteridentity.org/>
- [45] <https://medium.com/@ari.other/mapping-a-plan-to-improve-hardware-component-vulnerability-disclosure-5eca6f7a1938>
- [46] <https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5b4fe83b1ae6cfa99e58a05d/1531963453495/Better+Identity+Coalition+Blueprint+-+July+2018.pdf>
- [47] <https://ecs-org.eu/>
- [48] <https://www.interregeurope.eu/cyber/>
- [49] <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>
- [50] <https://www.dcypher.nl/nhtcu>
- [51] <https://ecs-org.eu/agenda>
- [52] <http://ecs-org.eu/membership>
- [53] <https://www.enisa.europa.eu>
- [54] https://europa.eu/european-union/about-eu/agencies/enisa_en
- [55] https://www.enisa.europa.eu/publications/corporate/enisa-strategy/at_download/file
- [56] <https://www.eitdigital.eu/about-us/action-lines/>
- [57] <https://www.eitdigital.eu/challenge/>
- [58] <https://www.eitdigital.eu/accelerator/>
- [59] <https://www.eitdigital.eu/>
- [60] <https://www.eitdigital.eu/newsroom/accelerator/all-news/scaleup-success-stories>
- [61] <https://ecs-org.eu/>
- [62] <https://mindthebridge.com>

- [63] <https://www.linkedin.com/school/mind-the-bridge-foundation/?originalSubdomain=it>
- [64] <https://mtsfund.co/>
- [65] <https://www.sec.gov/ocie/Article/ocie-about.html>
- [66] <https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf>
- [67] <https://www.sec.gov/info/complianceoutreach.htm>
- [68] <https://www.sec.gov/ocie>
- [69] <https://www.sec.gov/ocie/announcements>
- [70] <https://www.uscg.mil/home/>
- [71] <https://www.work.uscg.mil/Missions/>
- [72] <https://www.uscg.mil/Portals/0/Strategy/Cyber%20Strategy.pdf>
- [73] <https://safety4sea.com/uscg-initiatives-to-improve-cyber-security/>
- [74] https://www.uscg.mil/Portals/0/seniorleadership/alwaysready/USCG_Strategic%20Plan_LoRes%20Page_20181115_vFinal.pdf?ver=2018-11-15-140314-127
- [75] https://homeport.uscg.mil/Lists/Content/Attachments/2673/CG-5P%20Policy%20Letter%2008_16.pdf
- [76] [http://www.imo.org/en/OurWork/Security/Guide to Maritime Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%200\(Secretariat\).pdf#search=cyber](http://www.imo.org/en/OurWork/Security/Guide%20to%20Maritime%20Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%200(Secretariat).pdf#search=cyber)
- [77] https://www.work.uscg.mil/Portals/6/Documents/Resource%20Library/FY%202018%20Budget%20Overview_WEB%20FINAL.pdf?ver=2017-08-29-110735-463
- [78] https://www.uscg.mil/Portals/0/documents/budget/2019%20BIB_FIN_ALw.pdf



Quotation:

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

"Guidelines for Innovation Partnerships in Cybersecurity and Privacy for EU-US Collaboration. AEGIS project."

Consortium:

