RESEARCH IN FOCUS

How to Operationalise a Transatlantic Cyber Policy Research Initiative (TCPRI)

Julia Schuetze
Stiftung Neue Verantwortung
September 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Abstract

Three years after the European Union and the United States agreed on the launch of the Transatlantic Cyber Policy Research Initiative (TCPRI) as a key component for EU-US cooperation on cybersecurity policy, the provisions still remain largely theoretical. Taking up the idea for implementation, this paper considers current challenges and identifies why the TCPRI initiative is so relevant today. Additionally, it proposes how the TCPRI could be implemented, considering institutional setup, working methods and its relationship to policy-makers. Furthermore, this paper examines how the TCPRI's effectiveness could be augmented by a transatlantic strategy on cybersecurity policy research that applies elements of science diplomacy. Finally, it suggests ways the TCPRI could complement the existing ecosystem of cybersecurity policy research initiatives.

Key points

- The TCPRI's main objectives must be to foster research on cyber policy to tackle challenges of a constantly emerging threat landscape, study and analyse different cyber policy approaches in the US and EU to comparatively study the effect of differing cyber policy approaches to achieve cybersecurity and finally strengthen the capacity of stakeholders, such as civil society organisations, academia and think tanks, to work on cyber policy together across the Atlantic.
- Even though the TCPRI was mainly imagined as a research initiative for civil society, academia and think tanks, it should be inclusive for other stakeholders. When looking at some of the example cyber policy challenges (e.g. attribution, protection of critical infrastructure,) policy questions emerge and the data and information needed to answer them - cannot be tackled solely by think tanks, civil society and academic institutions because key information can only be found in government and the private sector. The institutional setup therefore needs to create access to information held by those stakeholders.
- The TCPRI's working method proposed in the paper aims to reveal policy options for diplomats that are scientifically informed.
- Building a common transatlantic strategy on cybersecurity policy research building on EU and US science diplomacy strategies could assist the TCPRI by making sure that the research, and the network itself, is used to its full potential.
- TCPRI should strengthen the ecosystem of already existing transatlantic cybersecurity initiatives. There is a number of organisations and people that have specialised on cyber diplomacy themes that EU-US diplomats deem important to tackle. The TCPRI should add to the ecosystem and provide some form of overarching connection with the purpose of specifically informing diplomatic efforts.

Disclaimer

This paper lays out a proposal for how the TCPRI can be implemented, while considering the institutional setup, working methods and conditions. Finally, it offers some recommendations that can support the research initiative in the long term. It leveraged the expertise and experience of cybersecurity researchers and other experts from the EU and the US. See here for further information about the Transatlantic Cyber Policy Research Initiative workshop which took place on 12 December 2018.

Introduction

It is in the EU's strategic interest to retain and develop essential capacities in order to secure its digital economy, infrastructure, society and democracy. Similarly, the United States is pursuing advances in cybersecurity that will thwart adversaries and strengthen public trust in cyber systems in order to preserve the Internet's growing social and economic benefits.[1] In EU and the US, cybersecurity research is an essential means to achieve these ends. Evidence of cybersecurity efficacy and efficiency, such as formal proofs and empirical measurements, drives progress in cybersecurity research and development and improves cybersecurity practice and governance. Funding and investment in cybersecurity research can be found in the EU's Horizon 2020 programme and in the US' Federal Cybersecurity Research and Development (R&D) Strategic Plan.[2] The US and the EU have a long history of successful cooperation in research in general;[3] for cybersecurity research, the "Agreement for Scientific and Technological Cooperation" started to simplify cooperation between US organisations and Horizon 2020 participants.

> **"Evidence of cybersecurity efficacy and efficiency, such as formal proofs and empirical measurements, drives progress in cybersecurity research and development and improves cybersecurity practice and governance.**

When looking at the research, areas of cybersecurity such as cybercrime are well more advanced than, for example, the issues of cyber diplomacy.[4] It hasn't been a priority on either side of the Atlantic in the last decade. Thus far in the EU Horizon 2020 program, cyber diplomacy and partnership research has received €25 million in funding, while social and ethical issues within cybersecurity have received €11 million. By comparison, the whole field of cybersecurity tools and management received €143 million and research topics for law enforcement received €60 million, according to a report by the European Court of Auditors.[5] In the US, the Federal Cybersecurity Research and Development Strategic Plan from 2016, which allocated funding for cybersecurity research, does not include the research field of cyber diplomacy at all.[6] Cybersecurity policy issues, however, especially in relation to cyber diplomacy, have gained importance. The EU has also recognized that cybersecurity policy increasingly shapes the international cybersecurity debate. Recent studies have identified a need for more US-EU collaboration on cybersecurity policy by assessing the current research landscape and identifying the biggest barriers to cybersecurity policy research cooperation. These barriers were primarily caused by "differences in policies and legislation on cybersecurity and privacy between the EU and the US, followed by the lack of coordination between funding programs in the US and Europe and the fragmented cybersecurity field between multiple communities".[7] Two of the recommendations are relevant for cyber diplomacy and cybersecurity policy, specifically: "To establish areas for collaboration that interest both the EU and

[1] Office of Science and Technology Policy (2016) Federal Cybersecurity Research and Development Strategic Plan, National Science and Technology Council, February 2016.

[2] See, The Network and Information Technology Research Program (2018) 2019 Federal Cybersecurity Research and Development Strategic Plan.

[3] European Commission (2019), International Cooperation USA Partners in Science: The EU at AAAS, European Commission, 18 February 2019.

[4] H. Carrapico & A. Barrinha (2018) European Union cyber security as an emerging research and policy field, European Politics and Society, 19:3, 299-303.

[5] European Court of Auditors (2019) Challenges to effective EU cybersecurity policy, page 24, European Court of Auditors, March 2019.

[6] Office of Science and Technology Policy (2016) Federal Cybersecurity Research and Development Strategic Plan, National Science and Technology Council, February 2016.

[7] AEGIS project (2019) Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation, page 22 Aegis, January 2019. and see also AEGIS project (2019) Policy Brief on Research and Innovation in Cybersecurity, Aegis, January 2019.

the US" and "to invest in international cybersecurity projects".[8] Research on cybersecurity policy that has a focus on cyber diplomacy can identify the EU's and US' sometimes diverging strategic approaches and their impact on transatlantic cooperation, identify the actors and processes that have shaped the policies, as well as suggest new forms of cooperation.

Background, Reasons and Objectives

The statement[9] following the 2016 EU-US Cyber Dialogue envisioned the launch of a Transatlantic Cyber Policy Research Initiative (TCPRI) as a key component for EU-US cooperation on cybersecurity policy. According to the document,[10] the goal of the TCPRI would be to "bring together European and U.S. civil society, academic, and think tank experts to address key cyber policy challenges, increase policy research capacity on cyber issues" and ultimately "aid both societies to be appropriately defended in the face of increasing malicious cyber activity by criminals, states, proxies, and terrorist organisations".[11] Beyond this declaration, so far the provisions remain largely theoretical. Meanwhile, several developments suggest that closer cooperation on cyber policy research between the EU and the US would be desirable now more than ever.

The constantly changing risk landscape

The cyber threat landscape is constantly changing.[12] The widespread use of narrow artificial intelligence is right around the corner and the Internet of Things continues to grow. Hardware and software vulnerabilities in existing, widespread products - as well as in Internet infrastructure - are creating weaknesses in defence. Moreover, attack tactics are adapting quickly.[13] Individually, neither the EU nor the US has a solution for the challenges that face their respective economies and societies. Staying up-to-date on the risk landscape is a challenge for government officials. Knowing which cybersecurity practices and governance structures should be prioritised in order to best manage risk is critical. Different stakeholders are needed to grasp these issues and develop policies that can build stronger defence. Therefore, tackling cybersecurity policy challenges with cybersecurity experts within the scope of a TCPRI is a prudent approach.

> **Individually, neither the EU nor the US has a solution for the challenges that face their respective economies and societies.**

> **Objective I:** Foster research on cyber policy to tackle challenges of a constantly emerging threat landscape.

[8] AEGIS (2019) White Paper on Research and Innovation in Cybersecurity, Aegis project, January 2019.
[9] European External Action Service (2016), EU-US Cyber Dialogue.
[10] European External Action Service (2016), EU-US Cyber Dialogue.
[11] European External Action Service (2016), EU-US Cyber Dialogue.
[12] ENISA (2019), ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, ENISA, January 2019.
[13] ENISA (2019), ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, ENISA, January 2019.

Cybersecurity governance approaches

The US and the EU have taken different approaches to cybersecurity policy domestically and internationally in the past. For example, to achieve greater cybersecurity of critical infrastructure, the US focused on implementing the NIST Framework whereas the EU passed the NIS Directive. These policies have the same end goal, but they try to achieve it with different policy tools. From a public policy analysis perspective, this creates room for case studies that could comparatively study the effect of differing cyber policy approaches to achieve cybersecurity. This can foster mutual learning in this constantly changing risk landscape and create an exchange over best practices for cybersecurity policy. Regulatory approaches for cybersecurity can have a cross-border effect, such as when international companies have to abide by the cyber policies of different countries, states or regions in which they are operating. A cyber policy research initiative can analyse the effects this has on the economy, societies and the open, secure and free Internet. When it comes to supply chain security, different cybersecurity governance approaches have already emerged. In the US, supply chain security initiatives include the NTIA's Software Transparency Initiative[14] and a ban on technology and services from "foreign adversaries" deemed to pose "unacceptable risks" to national security. These are the policy tools the US is currently using to create supply chain security nationally but with potential global effects.[15] In the EU, the Cybersecurity Act aims to create supply chain security through the creation of a Framework for the European Cyber Security Certification in consultation with a Stakeholder Cybersecurity Certification Group.[16] To that end, the TCPRI could be a way of studying the different approaches more closely and analysing what they mean for cybersecurity and the transatlantic relationship overall.

> “

A cyber policy research initiative can analyse the effects this has on the economy, societies and the open, secure and free Internet.

> **Objective II:** The study and analysis of different cyber policy approaches in the US and EU to better tackle current cyber challenges.

Building the capacity of academic and civil society stakeholders to strengthen the multi-stakeholder approach to cybersecurity governance.

Both the US and the EU support the multi-stakeholder approach to Internet Governance.[17] It has been recognised that for cybersecurity governance, "the effectiveness depends on cooperation among different stakeholders".[18] Multi-stakeholder initiatives exist to find solutions that foster the "synthesis of diverse knowledge and perspectives in a transparent and unifying decision-making process, engaging stakeholders with competing interests, perspectives, and agendas under uncertain and often adversarial conditions"[19]. This makes multi-stakeholder governance very complex and runs counter to other concepts of multilateralism and intergovernmentalism that focus on state sovereignty.[20] In cybersecurity

[14] M. Baksh (2018), Agencies anticipate results of NTIA software transparency work in efforts to secure supply chains, Inside Cybersecurity, November 2018.

[15] E. Feng (2019) U.S. move to isolate Huawei sends ripples through global supply chain, NPR Radio, May 2019.

[16] M. Schaffer (2018), European Cyber Security Certification ECSO Meta-Scheme Approach, European Cyber Security Organisation, March 2018.

[17] European External Action Service (2018) EU-U.S. Cyber Dialogue - Joint Elements Statement, EEAS, October 2019.

[18] C. Hoepers, K. Steding-Jessen, H. Faulhaber (2016) The Importance of a Multistakeholder Approach to Cybersecurity Effectiveness, NETmundial, 2016.

[19] Kambiz, Maani (2017) An Introduction to Multi-Stakeholder Decision Making. Multi-Stakeholder Decision Making for Complex Problems: pp. 3-14.

[20] Compare with W. Dutton, Multistakeholder Internet Governance? (2015), World Development report, May 2016: "In contrast, the MLg approach looks to governments as possessing the sovereign right to guide Internet policy and regulation, as they are the legitimate – elected – representatives of all actors within their respective nations", page 28.

governance, both the US and EU have put forth cyber policies that are driven by national security concerns. Those cyber policies can hurt objectives by other stakeholders and the stakes they have in an "open, secure and free Internet".[21] Striking a balance is no easy task. Back in 2015, NetMundial was already recommending that "governments, including military and intelligence sectors, in addition to traditional security and defence strategies, need to improve their awareness of the multi-stakeholder nature of the Internet and the vital importance of cooperation to address security threats".[22] By including civil society organisations, think tanks and academics, the TCPRI could be a vehicle for strengthening the voices of stakeholders who otherwise may not be heard, as they may not have the resources to take part in a discussion - or be invited to give feedback - about the effects of government cybersecurity policy on an open, free and secure Internet. Indeed, a prerequisite for a functioning multi-stakeholder approach is capacity-building. As Groß finds: "To enable effective representation of the interests of civil society, civil society should be supported in the long term, which includes assistance in networking and coordination, but also financial resources".[23] The TCPRI could strengthen the multi-stakeholder process by creating capacity for cybersecurity policy experts from different stakeholder communities (especially civil society and academia) that are organisationally not as well positioned as international companies or governments to formulate and voice their views on cybersecurity governance.

> **[...] a prerequisite for a functioning multi-stakeholder approach is capacity-building.**

> **Objective III:** Strengthening the capacity of stakeholders, such as civil society organisations, academia and think tanks, to work on cyber policy together across the Atlantic.

Institutional Setup

The institutional setup of a TCPRI is an important element to its success. Lessons from other multi-stakeholder initiatives can offer guidance as to what values should be reflected in the institutional setup of such an initiative.

An der Spuy (2017) finds that the following key values increase multi-stakeholder participation: inclusivity, diversity, collaboration, transparency, egalitarianism among different participants, flexibility and relevance, privacy and safety, accountability and legitimacy and responsiveness.[24] These values should be represented in the way the TCPRI is set up.

[21] G. Nojeim (2010) Cybersecurity and Freedom on the Internet.

[22] C. Hoepers, K. Steding-Jessen, H. Faulhaber (2016) The Importance of a Multistakeholder Approach to Cybersecurity Effectiveness, NETmundial, 2016.

[23] L. Groß (2018) Successfully Promoting Decentralisation: The Potential of the Multi-Stakeholder Approach, German Development Institute, February 2018.

[24] A. an der Spuy (2017). What if we all governed the Internet? Advancing multistakeholder participation in Internet governance. Other multi-stakeholder work process principles were outlined in the ECJ by Kasper and Shears (2018): A Multistakeholder Approach To Cybersecurity Policy Development, page 10-14.

Even though the TCPRI was mainly imagined as a research initiative for civil society, academia and think tanks, it should be *inclusive* for other stakeholders in order to broaden its access to expertise beyond those three main stakeholder groups (see Annex B). When looking at some of the example cyber policy challenges (e.g. attribution, protection of critical infrastructure,)[25] more stakeholders need to be included in some way. The policy questions - not to mention the data and information needed to answer them - cannot be tackled solely by think tanks, civil society and academic institutions because key information can only be found in different sectors. Therefore, TCPRI should consist of, or at least be *inclusive* of, other stakeholders, such as the private sector and the technical community. There needs to be formats that are *flexible* enough to engage these stakeholders. This can increase the *diversity* of participants involved but also make cyber policies more *relevant*, as solutions need be implementable. As part of this, consideration should be given to what kind of contributions are desired from the different stakeholders, e.g. share knowledge, provide feedback and expertise, research, organization of workshops, publications, media work or public engagements. The supporting structure and organisation of the TCPRI is an important basis for ensuring *transparency, legitimacy, collaboration and accountability* of the initiative. To achieve those values, the TCPRI will need a secretariat, a core group and a steering committee. To achieve the necessary flexibility and participation, the working method (discussed in more detail in the chapter "Working Method") calls for the TCPRI to be set up in such a way that it provides enough resources to embark on those policy questions in the first place. These resources should be both financial and personal. **A secretariat** should be able to assist with the coordination and preparation of workshops, meetings and papers, but should also be prepared to conduct research and scientific work on certain topics. Therefore, the secretariat should have expertise in data science to support the work of answering policy challenges. This can create legitimacy and accountability for research outcomes. The secretariat should be embedded in a hosting organization, a trusted third party (academic or think tank) that is non-partisan and has no political bias. The environment should be a *safe* space for discussion but at the same time be transparent enough so that stakeholders can follow decision-making processes well. The secretariat must always be transparent and *responsive* about its work. Workshops and community events should be private and safe. Target output should be the publication and presentation of policy options.

> **“**
>
> **[…] consideration should be given to what kind of contributions are desired from the different stakeholders […]**

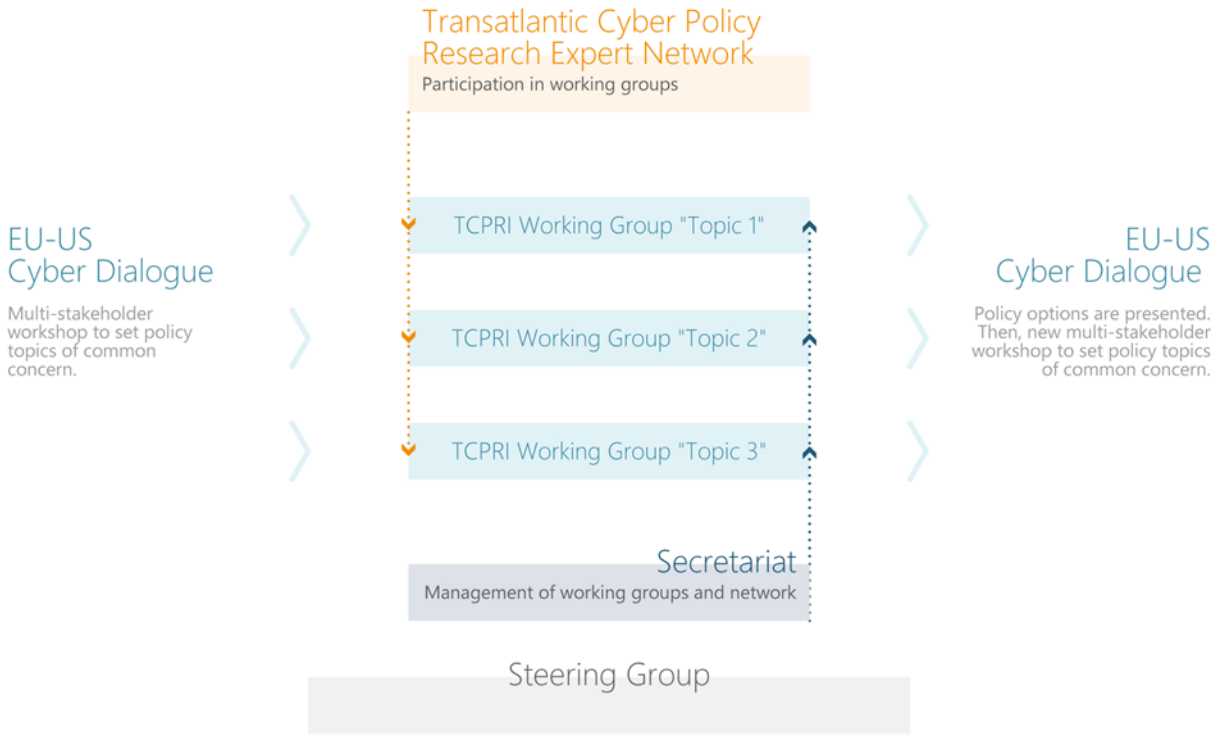
A **group of experts who make up the TCPRI network** would act as a knowledge base for the secretariat. Depending on the policy question at hand, the TCPRI members could be organised into **working groups** (see Figure 1 for the visualisation of a possible setup and working process).

The TCPRI members would be identified according to their expertise and position in the field. If expertise for a certain topic is missing in the network, then experts are added. The TCPRI should not be too large; instead, it should be a small, effective cell with wide independence and credibility that works with the secretariat to develop cyber policy options.

For more accountability over time, there could be some form of **Steering Group** that oversees the process and accounts for the work of the secretariat, the engagement of the TCPRI network and ultimately the relationship with diplomats and other decision-makers that may be target audiences. Contact with governments as stakeholders is important for the *relevance* of the TCPRI. In the next section, it is discussed how the TCPRI's cyber policy research could link to policy-making.

[25] which have been identified by workshop participants EU Cyber Direct (2018) Transatlantic Cyber Policy Research Initiative workshop, 12 December 2018.

Figure 1. Example Setup and Process of Transatlantic Cyber Policy Research Initiative



Linking Policy Research to Policy-Making

> **[…] cyber policy challenges and themes that diplomats have set during the EU-US cyber dialogue would be discussed and vetted by the group of experts that make up the TCPRI.**

In order to fulfil the goal of "addressing key cyber policy challenges",[26] the TCPRI would benefit greatly from some connection to policy-makers and current or former governmental experts. In order to identify current cyber policy challenges, the TCPRI needs to include - or at least have regular communication channels with - policy-makers in the EU and the US. This would make this initiative a true *policy* research initiative and avoid creating academic answers that do not address concrete policy challenges. Furthermore, including government policy-makers would give experts within the TCPRI an opportunity to share their views of how these policy challenges should be prioritised. One way could be through the **selection of challenges and joint prioritisation that TCPRI and policy-makers conduct together**. At the start of the cybersecurity policy research initiative, cyber policy challenges and themes that diplomats have set during the EU-US cyber dialogue would be discussed and vetted by the group of experts that make up the TCPRI. Members of the TCPRI would then add topics and exchange views on the importance and urgency of those topics. Since the overarching cyber diplomacy themes of the US and EU are quite broad,[27] the expert group may come up with more specific challenges than what the EEAS and its US counterparts decided on. This will make the research relevant for policy work from the start of each research project (working group). It will also enable expertise from within the transatlantic cybersecurity community, which deals with those subjects every day, to decide which challenge should be tackled first. Some form of exchange

[26] European External Action Service (2016), EU-US Cyber Dialogue
[27] European External Action Service (2018), Science Diplomacy

between the TCPRI and diplomats should be arranged throughout the process, as diplomats can add knowledge of essential day-to-day, practical challenges.

Working Method

TCPRI needs to be process-oriented as much as outcome-oriented to fulfil its objectives, e.g. tackling the constantly changing threat landscape. This should be reflected in the working style of the TCPRI. It is therefore important to consider the process of how TCPRI comes to its conclusions and creates cyber policy research outcomes. Here, researchers from the University of Tufts came up with a work-flow model that can support policy research and that creates outcomes which can be considered by policy-makers. They called this concept "informed decision support", which manifested in a step-by-step decision tree. The decision-support process is designed to reveal policy options for diplomats that are scientifically informed. The process allows flexibility as during the different phases the group can adjust iteratively in response to changing circumstances. Thus the emphasis is process- and outcome-oriented. The ultimate goal - options that lead to informed decisions - can then be used or ignored explicitly on the political level (Tufts University, 2018).

> **Informed decision support is a useful method for international policy research when countries have competing interests.**

This research process is especially interesting as it aims to balance national interests with common interests (i.e. national security goals and civil liberties goals), which is one of the main challenges of cybersecurity when competing stakes meet. It can also be a useful method for international policy research when countries have competing interests, for example. This decision-support process is necessarily international, interdisciplinary and inclusive, according to researchers who have seen the process applied in other policy fields. The benefits would become clearer if the process were applied using these steps:

Step 1: Identification of a common concern

One of the challenges identified by diplomats and TCPRI together, such as resilience, is analysed according to *common concerns*. A common concern could be, for example, the lack of a common definition and framework for resilience that prevents the EU and US from working on this issue together effectively. It could also be the lack of a good and common understanding of hybrid threats or risks.

Step 2: Identification of specific policy questions that need answering in order to address the common concern

The second task in the process is to *identify specific policy questions that need answering in order to address the common concerns*. While identifying questions of common concern, appropriate methodologies can be identified. Questions of common concern could be, for example, "How can we set up a sustainable dialogue about multiple threats and vulnerabilities?" or "What are common instruments to achieve resilience?" Once those questions are identified, the TCPRI can start looking for information and observations that are then organised and analysed as data. Challenges, as with every other research endeavour, might be that the required data may not exist yet or that data is spread across different stakeholder groups. Therefore, it is imperative that the TCPRI can work flexibly while also having enough support to gather and access specific data (see Annex A). Evidence, resulting from the integration of data and governance mechanisms, alerts decision-makers to the need for action and provides an empirical basis for good policies.

Step 3: Data and information gathering to create policy options

By using the data and information, so-called options are developed. Options in the context of TCPRI could be policies, regulations, cooperation, etc., that address the policy questions discussed, while being

supported by data and information. Options are the basis for policy-makers or diplomats to make informed decisions. Or, to put it more simply: The main contribution of research is to deepen the analysis and provide policy-makers with a wider menu of options and an estimate of their respective (positive and negative) implications. The whole point of research is to deepen the policy discussion and improve the basis for decision-making. Options subsequently frame the specifications for decisions about governance mechanisms (including policy and regulatory devices) and build infrastructure (involving technology and capitalisation), which are required together to achieve sustainability. So options could already be revealed during the research phase.

The process envisions a flexible research environment that allows options to emerge as data and information are collected to address policy questions. This gives policy-makers a more scientific understanding of how to tackle challenges, makes them aware of different approaches (options) they could take and builds the basis for further political discussions that are supported by data and information.

Supporting Actions for TCPRI

To support the TCPRI, there are two ideas which would strengthen the initiative and make it more sustainable. The first is building a common EU-US science diplomacy strategy for the TCPRI and including the TCPRI in the existing cyber policy research ecosystem.

Creation of a Transatlantic Cybersecurity Policy Research Strategy

Building a common transatlantic strategy on cybersecurity policy research building on EU and US science diplomacy strategies could assist the TCPRI by making sure that the research, and the network itself, is used to its full potential. To that end, it is useful to look at what science diplomacy means and how it is currently used in the US and EU.

In the 21st century, diplomacy is not only monopolized by states but also extends to non-state actors, including NGOs, private companies and academia. The most influential companies are technology-driven; travel is cheap; and scientific work is globalised. It is worth establishing what role the private sector, academia and civil society can play in diplomacy. Here, the concept of science diplomacy can help. The term "science diplomacy" was coined by the first book in this new field,[28] emerging as it did from the 2009 Antarctic Treaty Summit[29]. "Science Diplomacy is an emerging strong tool for diplomacy and foreign policy, and is often based on the countries' principal objectives and interest to address common problems as they build constructive international partnerships"[30]. The EU[31] and the US[32] are already using forms of science diplomacy, but not necessarily for cybersecurity policy. Berkman, a science diplomacy scholar and practitioner, said "people usually think of diplomacy as how states represent themselves and negotiate to advance their own interests. These are the fraught high-level talks between nations that are featured on newspapers' front pages".[33] Berkman proposes that science diplomacy can instead be a common denominator for tackling cross-border issues, as different

[28] Berkman (2011), Science diplomacy : science, Antarctica, and the governance of international spaces https://repository.si.edu/handle/10088/16154

[29] The Antarctic Treaty Summit: Science-Policy Interactions in International Governance (2009)

[30] Cartey, 2018 in RIS (2018:58), South-South Cooperation: Role of Science Diplomacy

[31] Directorate-General for Research and Innovation (European Commission) (2017), Tools for An EU Science Diplomacy and European External Action Service (2018), Science Diplomacy https://eeas.europa.eu/topics/science-diplomacy_en

[32] U.S. State Department (2008) Science Diplomacy and the U.S. Department of State and Turekian (2016), The Role of Science Diplomacy in International Crises; Syria as a Case Study https://2009-2017.state.gov/e/stas/2016/260459.htm

[33] Berkman (2018), Could science diplomacy be the key to stabilizing international relations?

disciplines of science can reveal common interests that could be the basis for negotiation - and may be less politically charged.

In another example, the inclusion of technical experts has already advanced international cooperation on cybercrime and set higher security standards.[34] This shows how much potential lies within science diplomacy. It is, however, important to determine which form of science diplomacy would be particularly useful and promising for EU and US cyber diplomacy. There are different formats of science diplomacy, and although they can overlap, it makes sense to consider them separately.

Firstly, **diplomacy for science** is mainly about facilitating international scientific collaboration. Here, classic tools of diplomacy are used to support the scientific and technological community. Diplomacy is employed to establish cooperation agreements on a government or an institutional level. The goal of diplomacy for science is to benefit from foreign science and technology capacity in order to improve a state's national capacity.

Secondly, **science for diplomacy** is when scientific partnerships can improve international relations. It draws on the universal language of science to engage countries, reinforce relationships and ease tensions in situations of political strain.[35]. Practically, this could be a network of people who still engage in joint projects when political relations are strained or limited[36]. In cybersecurity policy, science for diplomacy can create a strong network of stakeholders that work on cybersecurity policy challenges.

Thirdly, **science in diplomacy** is when science informs diplomacy. In times of peace, this is about using scientific knowledge in foreign policy decisions. The goal of such activities is to improve foreign policy actions through scientific knowledge. Soler puts it this way: "Science in diplomacy is the direct input of science into diplomatic discussions and agreements, and into the formulation of foreign policy"[37]. This can mean proposing evidence-based solutions and ways forward, but also the inclusion of scientists at the diplomatic table. In transatlantic cybersecurity policy, science in diplomacy could assist in creating better attribution, for example, through the sharing of specific data - and therefore determining joint diplomatic responses.

> **Science diplomacy is most effective when it is guided by a coherent strategy.**

Science diplomacy is most effective when it is guided by a coherent strategy. Indeed, the most efficient way to maximize researchers' productivity is for policy-makers to decide beforehand which cybersecurity challenges would benefit from the inclusion of non-governmental stakeholders. This then creates what is known as a "focus of effort" among researchers, since they know which topics could have a potential impact - and need not waste their time looking at topics policy-makers already know they will ignore.[38]

The Directorate-General for Research and Innovation has found that, "Today, Science Diplomacy is already mentioned as one of the policy domains of the EEAS (European External Action Service), but it is not central to its strategy"[39]. They argue that "the actual and potential role of S&T [science and technology] in the functioning of the EEAS" still needs to be defined. In the United States, there is a long history of science diplomacy. Most recently, in May 2016, the Committee on Homeland and National

[34] Waldron (2017),Experts Call for International Collaboration on Cybersecurity Issues

[35] American Association for the Advancement of Science (2018), Science Diplomacy: An Introduction

[36]Krasnyak (2018), The Apollo–Soyuz Test Project: Construction of an Ideal Type of Science Diplomacy http://booksandjournals.brillonline.com/content/journals/10.1163/1871191x-12341028

[37] Soler (2017), Science Diplomacy: An Introduction (Video) https://www.youtube.com/watch?v=E9RFLD_FM6A

[38] Gluckman, V. Turekian, R.W. Grimes, and T. Kishi, "Science Diplomacy: A Pragmatic Perspective from the Inside," Science & Diplomacy, Vol. 6, No. 4 (December 2017) http://www.sciencediplomacy.org/article/2018/pragmatic-perspective

[39] Directorate-General for Research and Innovation (European Commission) (2017), Tools for An EU Science Diplomacy https://publications.europa.eu/en/publication-detail/-/publication/e668f8cf-e395-11e6-ad7c-01aa75ed71a1

Security of the National Science and Technology Council issued a strategic document called, "A 21st Century Science, Technology, and Innovation Strategy for America's National Security". This report proposed a strategy on how the S&T community should evolve to address the challenges facing it. Science diplomacy is operationalised by fellowship programs, for example. An effective use of science diplomacy in cybersecurity policy and in the US and EU diplomatic work would therefore have to reflect the goals of both partners. These goals would have to be supported by a strategy, but they would also have to be operationalised in such a way that they could assist political decision-makers to make an informed decision. The decision-support process is designed to reveal options (without advocating for one or the other), which can be used or ignored explicitly. This contributes to informed decision-making by nations individually and collectively[40].

TCPRI can play a significant role in science diplomacy between the EU and US. EU Commissioner Carlos Moedas, the European Union's Commissioner for Research, Science and Innovation, has taken a dedicated stance on the relevance of science and research that could inform diplomacy. He has outlined this especially in reference to transatlantic relations. According to Moedas, "The US and EU are not only instinctive and effortless partners on scientific endeavours", but "make very natural allies" as "we are confronted by the same struggles, science diplomacy presents a matchless opportunity to address the political, demographic and environmental challenges of the age through universal language and expression of scientific endeavours"[41]. The US State Department also sees science as an important aspect for diplomacy: "Science engagement is an indispensable tool of U.S. diplomacy to build relationships and strengthen ties with countries and regions viewed as foreign policy priorities"[42]. Since the concept of science diplomacy can have different meanings, and understandings of what science can do for diplomacy may differ, it is useful to have a strategy that informs scientific endeavours and allows for the setting of goals. If endeavours among two or more countries are pursued, it is beneficial to align strategies or create a common strategy. The State Department, for example, seems to put emphasis on science as a way to build relationships, whereas the European Commission also sees it as a means for collectively addressing challenges. Here, expectations of what a TCPRI should achieve may clash. A common strategy for transatlantic cyber research initiatives could focus on "low hanging fruits" for collaboration and common concern challenges and through this, build networks and trust as well as expertise. *A starting point is also to look at the EU's internal use of science diplomacy for cybersecurity challenge.*[43]

Integration in the cybersecurity ecosystem

The TCPRI should strengthen the ecosystem of already existing transatlantic Cybersecurity initiatives. There is a number of organisations and people that have specialised on cyber diplomacy themes that EU-US diplomats deem important to tackle. Not all of them are necessarily connected or know of each other. Therefore, it makes sense to really find the right stakeholders to be added to the TCPRI. Last but not least, when thinking about setting up the TCPRI, it should be considered how the initiative may add to the ecosystem and provide some form of overarching connections with the purpose of specifically informing diplomatic efforts. This is why the institutional set-up could see the TCPRI more as a network which is supported by full time staff in a secretariat rather than a group of researchers that make up the TCPRI for one research project. This allows not only to seek people that have recognition in the community and have been working on those issues for a while, but also gives opportunities to flexibly build working groups on specific topics while ensuring the work itself is not too time-consuming for individual experts in different fields.

[40] Tuft University (2018), Science Diplomacy https://sites.tufts.edu/sciencediplomacy/about/science-diplomacy/
[41] C. Moedas (2015), "The EU Approach to Science Diplomacy." : 1–3.
[42] U.S. Department of State (2019), Key Topics – Office of the Science and Technology Advisor.
[43] Researchers from the Horizon2020 project S4D4C are currently building cases for how the EU uses science diplomacy internally that could be used as guidelines. More on their analysis of EU science diplomacy here.

Next Steps

If the EU and US were to pursue the endeavour of a Transatlantic Cyber Policy Research Initiative, the first step would be to set up a steering group and a lightweight secretariat. The steering group would engage with EEAS and US diplomats to reaffirm the commitment to the idea - potentially as talking point in the 2019 EU-US cyber dialogue. The secretariat's first task would be to analyse the ecosystem and identify where to host the TCPRI. The second step would be to appropriately equip the secretariat with resources while organising an interdisciplinary EU-US workshop - in lieu of the EU-US cyber dialogue - that would identify concrete policy challenges and ensure that they align with EU and US strategies. The third step would then be the setup of corresponding policy working groups. Running in parallel to those three steps, it would facilitate the success of the initiative if the EEAS were to review and potentially consolidate its strategic approach towards science diplomacy.

Annexes

A. Application of Decision-Making Tree During TCPRI Workshop "Resilience" on 12 December 2018 in Washington, DC

Step 1) Identify Common Concerns of EU and US Applied to the Topic of Resilience	Step 2) Specific Policy Questions That Emerge From Common Concern "Lack of Common Framework and Definition of Resilience" and "Lack of Understanding of Hybrid Threats/Risks" Identified in 1)
> Lack of awareness > Lack of harmonisation > Lack of common framework and definition of resilience > Lack of consensus of threat landscape > Lack of common criteria/market framework/liability > Lack of understanding of hybrid threats/risks > Lack of strategic communications	> What are channels for understanding those risks? > How can we concentrate more on prevention and response? > How can we set up a sustainable dialogue about multiple threats and vulnerabilities? > How can we identify and leverage already existing dialogues on resilience? > What can policies that operationalise resilience look like? > How can the public sector engage with industry on resilience? > What are policies that would organise EU/US resilience? > What are common criteria of resilience? > Do we include only cybersecurity exclusively or does the resilience definition include other domains, such as education, society, economy? > What is more effective PPP or regulation: NIS versus NIST effectiveness
Step 3) Data E.G. Information and Observations Needed to Answer Policy Questions Identified in 2)	**Step 4)** Stakeholders Perspectives Needed to Answer Questions 2) and Gain Data/Information Identified From 3)
> EU-US regulatory framework/relative effectiveness > Data on effectiveness of actions of government, industry > Taking data of the tech landscape > Legal frameworks and degrees of adoption > Gathering industry/civil society/government view on resilience and the components (prevention) > Threat/vulnerability data "dynamics of the threat environment" > Cyberattack incidents and development > Expert assessments > Reliance on ICT infrastructure	> Cyber Threat Intelligence Companies, Social Media Providers, CERTs, CSIRT Network > Cloud Service Providers/ISPs, Europol Critical Infrastructure Operators, Regulators Bodies > Intel/LEA Communities, Academia (interdisciplinary) > S&T community, Business association/Chamber of Commerce > Parliaments, Cybersecurity Agencies > Consumer Associations > Insurance Companies > MNC, National Statistical Agencies

- Cybersecurity indexes
- Social media data

- Investigative Journalists, Diplomacy Community
- Military

B. Non-Exhaustive List of Possible Stakeholder Groups Within the TCPRI

- Cyber Threat Intelligence Companies
- Civil Society Organisations
- Social Media Providers
- Computer Emergency Response Teams (CERTs)
- Computer Security Incident Response Network (CSIRT Network)
- Cloud Service Providers / Internet Service Providers (ISPs)
- Europol
- Critical Infrastructure Operators
- Regulatory Bodies
- Intelligence and Law Enforcement Communities
- Academia (interdisciplinary)
- Science and Technology Community
- Business Associations / Chamber of Commerce
- Parliaments
- Cybersecurity Agencies
- Consumer Associations
- Insurance Companies
- Multinational Corporations (MNCs)
- National Statistical Agencies
- Investigative Journalists
- Diplomatic Community
- Military

About the author

Julia Schuetze works on cyber diplomacy of the European Union with the United States and Japan as part of the EU Cyber Direct project. She also works as project manager of the "Transatlantic Cyber Forum" which deals with international cyber security policy. Her research focus is on cyber operations against electoral processes, comparative cybersecurity policy and governance. As part of her role at SNV she has spoken at the Congressional Cybersecurity Caucus in the United States, has facilitated workshops on Germany's cybersecurity architecture with the foreign office, has organized the cybersecurity conference with the Bundesakademie für Sicherheitspolitik as well as several other workshops and events with U.S. and German cybersecurity experts in Washington D.C. and Berlin. Her work has been published or cited by news outlets, such as WirtschaftsWoche Der Tagesspiegel, F.A.Z and the BBC. She is a Cybersecurity Policy Fellow at New America Foundation and volunteers for the OGP Civil Society Working Group and for the Steering Committee of the Internet Governance Forum Germany.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.