3. Cyber Security: Mapping the Role of Science Diplomacy in the Cyber Field

Authors:

Lucie Kadlecová, Nadia Meyer, Rafaël Cos, Pauline Ravinet

Cite as:

Kadlecová, L., N. Meyer, R. Cos, P. Ravinet (2020): Cyber Security: Mapping the Role of Science Diplomacy in the Cyber Field. In: Young, M., T. Flink, E. Dall (eds.) (2020): Science Diplomacy in the Making: Case-based insights from the S4D4C project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 770342.

List of Abbreviations

Czech Republic:	
MU	Masaryk University
MFA	Ministry of Foreign Affairs of the Czech Republic
NATO	North Atlantic Treaty Organisation
NCISA	National Cyber and Information Security Agency
NCSC	National Cyber Security Centre
NSA	National Security Authority
PROPED	Projects of economic diplomacy
TA ČR	Technology Agency of the Czech Republic
Germany:	
FOC	Freedom Online Coalition
France:	
ANSSI	National Cybersecurity Agency
CAPS	Centre for Analysis, Forecasting and Strategy
COMCYBER	Cyber military command
DGA	Weapons Directorate
FRS	Foundation for Strategic Research
GDRIS	International and Strategic Affairs Directorate
GGE	United Nations Group of Governmental Experts
IFRI	French Institute for International Relations
INRIA	National Research Institute for the Digital Sciences
IRIS	Institute for International and Strategic Affairs
IRSEM	Military School Institute for Strategic Research
MEAE	Ministry for European and Foreign Affairs
SGDSN	General Secretariat for Defence and National Security
European Union	
CFSP	Common Foreign and Security Policy
EEAS	European External Action Service
ENISA	EU Agency for Network and Information Security
EU	European Union
EU ISS	EU Institute for Security Studies
GMF	German Marshall Fund of the US

H2020	Horizon 2020
ICT	Information and telecommunication technologies
NIS Directive	Directive on Security of Network and Information Systems
SNV	Stiftung Neue Verantwortung
TCPRI	Transatlantic Cyber Policy Research Initiative
DG Home	Directorate General for Migration and Home Affairs
DG CNECT	Directorate General for Communications Networks, Content and Technology

1. Introduction

Cyber security topics have been part of national defence discourses for more or less the past thirty years. With a growing number of cyber attacks originating in one state and targeting another, cyber security has slowly entered the agenda of international community as well. The discussion has mainly been concerned with technology and technical solutions, but as the topic has gained greater attention, it is now being addressed by the world of international diplomacy. Nowadays, the role of cyber security in diplomacy has become so important that the term "cyber diplomacy" has come into global use, and countries are even deploying their own "cyber diplomats".

This report uses three important terms that must be explained at the beginning, especially if the reader is a newcomer to issues of cyber space. Firstly, the term "cyber security" is often used throughout this report. There is no single definition of the term. Each nation-state defines for itself what cyber security means. More than one definition of cyber security can be in use within a single state, because different national agencies and institutions may deal with different aspects of cyber security. Thus, the definition of the term in an organisation that focuses on industrial control systems is probably different from the one used by an organisation concerned with, for example, cloud security. Yet, if the organisations' individual definitions are studied closely, one will likely come to the conclusion that cyber security is the state of readiness of an organisation's services or systems, as well as its planning for recovery of functions if and when a breach of security occurs.

The second term which must be clarified is "cyber defence". Again, no commonly agreed definition of cyber defence exists, but certain common elements can be observed. Cyber defence covers a narrower spectrum of activities than cyber security. It refers to activities that protect a state from advanced hostile attacks undermining its integrity, sovereignty and national interests. These kinds of attacks are often conducted on a massive scale and can seriously threaten a state's ability to defend itself against external threats. Cyber defence enters the picture when cyber attacks cannot be handled by the traditional measures and tools of cyber security.

Finally, the third commonly used term is "cyber diplomacy". This term is probably the least controversial or confusing because it simply refers to applying traditional diplomatic tools and measures to international issues arising in the cyber domain. Of the three terms, cyber diplomacy is the newest concept. It is now recognised and employed by states around the world.

Given how new these terms are, the goal of this report is to map the landscape of cyber security and cyber diplomacy in the Czech Republic, Germany, France, and the EU and explore how those three states and the EU approach science diplomacy in the cyber realm. The cases briefly touch upon the historical background and explore the landscape of stakeholders. Later, they illustrate governance in practice, that is, how the optimal theoretical set of governance arrangements is reflected in practice. Finally, the report offers a meta-perspective of science diplomacy in the area of cyber security and identifies common features of the cases studied.

The research team worked with two main sources of information which were interviews and documents. Interviewees represented stakeholders from both government and academia. All the interviews were anonymous, citing only the interviewee's organization and time and place of the interview. Furthermore, the research team worked with various official documents ranging from government strategies and white papers to press releases and official statements as well as other texts such as active webpages of the discussed projects.

2. Czech Republic's Approach to Science Diplomacy in Cyber Space

2.1. Governance Arrangement

The history of cyber security in the Czech Republic dates back to 2011, when the Czech National Security Authority (NSA) was appointed as the national authority for the cyber agenda. A year later, the NSA published the first ever *Cyber Security Strategy of the Czech Republic for 2012 to 2015* which set the goal of creating the National Cyber Security Centre (NCSC) as part of the NSA. The NCSC was officially opened in May 2014. It is the main coordinating body for cyber security in the country. Since then, cyber security in the Czech Republic has progressed immensely. The proof of that is the latest National Cyber Security Strategy, for the period from 2015 to 2020, which sets forth the country's desire "to play a leading role in the cyber security field within its region and in Europe".[1] To fulfil such an ambitious goal, an independent National Cyber and Information Security Agency (NCISA) was created in August 2017. The NCISA replaced the NCSC, adopting the NCSC's agenda and boosting its capabilities and capacities.[2]

As part of that process, cyber diplomacy had to be strengthened, especially after January 2017, when the Czech Ministry of Foreign Affairs (MFA) detected a serious cyber campaign directed against its own computer networks.[3] The first and, so far, the greatest milestone in the development of Czech cyber diplomacy was the deployment of three Czech "cyber attachés" to Washington, D.C., Brussels and Tel Aviv in 2016. All three cyber attachés are employees seconded from the NCISA.

When it comes to science diplomacy, the Czech Republic has two science diplomats who are employees of the MFA, one in Washington, D.C. and one in Tel Aviv. In general, there is no specific, explicit strategy for the country's cyber diplomacy and science diplomacy. The only document that does touch upon cyber diplomacy and the ongoing research in the domain is the *National Cyber Security Strategy for the Period from 2015 to 2020*. Among its goals, the *Strategy* includes "active international cooperation" focused on engagement in international fora such as the EU and NATO, promotion of cyber security in Central Europe, and deepened bilateral cooperation with partners.[4] The crucial part of the document for science diplomacy is the goal of strengthening "research and development/consumer trust" which is to be achieved by participation in national and European research projects, appointment of a national cyber security coordinator as the main point of contact for research in the area of cyber security and encouragement of cooperation with academia and the private sector on research projects at the national, international, and transatlantic levels.[5]

Improvement of transborder cyber security through diplomacy and research is mentioned in the margins of some other strategic documents. One of them is the *Interdepartmental*

[1] National Security Authority, National Cyber Security Centre (2015): National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. p.7, Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf

[2] For more details on the history of development of cyber security in the Czech Republic, please, see Kadlecová, Lucie, Daniel Bagge, Michaela Semecká, Václav Borovička (2017): The Czech Republic: A Case of a Comprehensive Approach toward Cyberspace. Tallinn: NATO CCDCOE. Retrieved from: https://ccdcoe.org/library/publications/the-czech-republic-a-case-of-a-comprehensive-approach-toward-cyberspace/

[3] Interview, Ministry of Foreign Affairs of the Czech Republic, Prague, 5 December 2018.

[4] National Security Authority, National Cyber Security Centre (2015): National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. p. 17, Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf

[5] National Security Authority, National Cyber Security Centre (2015): National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. p. 19, Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf

Concept of Support for Security Research of the Czech Republic which was published by Ministry of Interior. It sets forth the national approach to security and innovation for 2017 through 2023, and mentions cyber security in that connection.[6] Furthermore, the document states an intention to prepare an action plan for use of economic and science diplomacy tools in order to develop better contacts with the main stakeholders in security research in the region (point C.3.2). However, it does not specify what those tools are. It prioritises the USA, Israel, the UK, Switzerland and the Scandinavian countries as the main partners for cooperation.[7] This is probably the first document that has mentioned a strategic framework for science diplomacy in the security domain.[8]

Another example of a document that addresses a need for strengthened international scientific cooperation is the *National Research, Development and Innovation Policy of the Czech Republic 2016–2020*. That policy was approved by the Czech Government in February 2016. It briefly mentions cyber security research.[9] To sum up, although there are strategic documents which suggest that the will exists on the part of Czech public authorities to develop science diplomacy for cyber security, the Czech Republic has no express, coherent cyber diplomacy or science diplomacy strategy at the time of writing this report in spring 2019.

2.2. Stakeholders

The key stakeholder in cyber security in the Czech Republic is the NCISA, which so far has most of the expertise and experience in cyber diplomacy (and possibly also overlapping into science diplomacy). The NCISA has by default been the country's key actor in cyber diplomacy and relations with academia, both because of its policy remit and also because there is no other entity capable of taking over responsibility for diplomatic relations in cyber security.[10] The NCISA is the agency that supplies Czech cyber attachés to the field. In 2016, three cyber attachés were posted to Tel Aviv, Washington, D.C., and Brussels. In the future, NCISA will decide on the distribution of funds received from the European cyber security competency centres and network.

Another actor that is gaining importance is the Ministry of Foreign Affairs. So far, the MFA has not been much involved in cyber diplomacy, but it has the intention of getting more active in the near future. That intention is reflected in its appointment of a Special Envoy for Cyber Space and the establishment of a Cyber Security Department. Ideally, the MFA and NCISA should complement each other—NCISA would articulate positions on cyber security-related issues which the MFA would then advocate abroad during diplomatic negotiations.[11] As it stands now, the MFA's capabilities are limited, which means that it is mainly NCISA that coordinates the Czech Republic's cyber diplomacy. However, as far as science in general is concerned, the MFA has posted two of its employees as science diplomats in Tel Aviv and Washington, D.C. Besides that, the MFA organises economic diplomacy projects (PROPED), which involve sending trade missions abroad. Although the MFA's primary goal is to support the business sector, there are also opportunities for it to get involved with academia. In the eyes of the MFA, science diplomacy, especially that

[6] Ministry of the Interior of the Czech Republic (2017): Interdepartmental Concept of Support for Security Research of the Czech Republic. Retrieved from: https://www.mvcr.cz/vyzkum/clanek/koncepce-meziresortni-koncepce-podpory-bezpecnostniho-vyzkumu-cr.aspx

[7] Ministry of the Interior of the Czech Republic (2017): Interdepartmental Concept of Support for Security Research of the Czech Republic. Retrieved from: https://www.mvcr.cz/vyzkum/clanek/koncepce-meziresortni-koncepce-podpory-bezpecnostniho-vyzkumu-cr.aspx

[8] Interview 4, NCISA, Prague, 26 March 2019.

[9] Government of the Czech Republic (2016): National Research, Development and Innovation Policy of the Czech Republic 2016–2020. Retrieved from: https://www.vyzkum.cz/FrontClanek.aspx?idsekce=782691

[10] Interview 2, NCISA, Brno, 17 January 2019.

[11] Interview 2, NCISA, Brno, 17 January 2019.

related to cyber security, is considered closely related to or perhaps even an indispensable part of economic diplomacy.[12] An example was a PROPED mission to the UK, where an NCISA representative had an opportunity to establish contacts with universities in London.[13] In 2019, two PROPED missions focused on cyber security are planned for India and the USA.[14]

CzechInvest is another important stakeholder in science diplomacy and cyber security. It is the Czech business and investment development agency and is subordinate to the Ministry of Industry and Trade. It promotes both domestic and foreign investment into the Czech Republic. CzechInvest's role is unique because of its knowledge of the Czech academic environment and local practice in various disciplines. It applies that knowledge to organise missions abroad that are specialised in selected industries. For example, CzechInvest organised a mission to Canada in September 2018 with a special focus on artificial intelligence. Canada aims to be a showcase of artificial intelligence. The main goal of this particular mission was to promote Prague as a future knowledge hub for the industry that would be of great interest to Canadian firms.[15]

The other stakeholders involved in cyber security and research play a rather marginal role. The Technology Agency of the Czech Republic (TA ČR) is one of them. Although TA ČR is not primarily oriented toward foreign countries, an exception to the rule is its Delta Programme, which supports international cooperation in experiment-based development and applied research.[16] The Ministry of Interior is a stakeholder thanks to the research it is doing in the field of security. So is the Ministry of Industry and Trade, because its representatives in Czech embassies often participate in diplomatic activities oriented towards further developing Czech expertise and commerce in cyber security and other sciences.[17]

Finally, the academic community, including all major Czech universities such as Charles University, the Czech Technical University and the Technical University in Brno cannot be ignored. In particular, Masaryk University in Brno has an especially strong position in science diplomacy and cyber security because of its close cooperation with the NCISA. However, Masaryk University does not contribute much directly to international science diplomacy because the focus of its cooperation is on domestic issues.

Overall, the structures and activities of stakeholders in science diplomacy and cyber security in the Czech Republic are not well-defined and perhaps even downright confusing. It often happens that one stakeholder does not know about the activities and opportunities developed by another actor in the same area.[18] More intense cooperation between the ministries and other government bodies, which could potentially result in the creation of coordinated structures and strategies, is lacking.[19]

[12] Interview, CzechInvest, Prague, 29 November 2018.

[13] Interview 3, NCISA, Prague, 26 March 2019.

[14] Ministry of Foreign Affairs of the Czech Republic: Projects of Economic Diplomacy for 2019. Retrieved from: https://www.mzv.cz/ekonomika/cz/servis_exporterum/projekty_ekonomicke_diplomacie/projekty_ekonomicke_diplomacie_pro_rok.html

[15] Interview, CzechInvest, Prague, 29 November 2018.

[16] Technology Agency of the Czech Republic (2018): Programme Delta 2. Retrieved from: https://www.tacr.cz/index.php/en/26-programy/delta/1469-delta-delta-2-guidepost.html

[17] Interviews 3 & 4, NCISA, Prague, 26 March 2019.

[18] Interviews 3 & 4, NCISA, Prague, 26 March 2019.

[19] Interview 2, NCISA, Brno, 17 January 2019.

2.3. Governance Practice

So far, cyber security has played only a marginal role in the Czech Republic's science diplomacy. Therefore, there have been only a handful of projects and activities in this area. Such activities as there have been were organized on a rather random basis, to take advantage of one-off opportunities. One of the first activities in the area was an application by NCISA to participate in the NATO Science for Peace and Security programme in 2016/2017. NCISA offered to organise a workshop on monitoring computer network operations, in cooperation with Israeli partners in government and academia. Although the application was unsuccessful, it was an important first test of NCISA's ability to cooperate with the Czech Republic's science diplomat and cyber attaché in Tel Aviv.[20]

Another project, in which NCISA gained its first experience with science diplomacy in the cyber sphere was the NATO Multinational Cyber Defence Education and Training project, which ran from 2014 to May 2019. The goal of the training project was to tap into the knowledge held by NATO members in order to devise new initiatives for NATO and its members in the areas of cyber defence training and education. Among those initiatives were new courses on cyber intelligence, development of cyber defence capabilities and Master's degree programmes on cyber defence and cyber security law.[21] Besides NCISA, Masaryk University was also invited to contribute to development of the curricula for the courses. Although the project had great ambitions, both of the Czech participants agree that the project was rather unsuccessful due to the lack of strong management by the project's leadership.[22] On the other hand, the project demonstrated smooth cooperation between NCISA and Czech academia.[23]

Other projects similar to those realized by NCISA include the activities of Masaryk University (MU). For example, representatives of its Institute of Law and Technology serve as observers to the UN Commission on International Trade Law and the UN Office on Drugs and Crime. They were requested to participate in the trade law meetings by the Czech Ministry of Industry and Trade and in the latter meetings by the UN Office on Drugs and Crime itself. Both sets of meetings dealt with elements of cyber security. The Czech academic observers contributed input to policy documents.[24]

Another promising form of science diplomacy that involves a cyber element is possible future cooperation between MU and Georgetown University. Georgetown has developed a programme for supporting research and cooperation on cyber issues, which MU would like to launch in the Czech Republic. This is still in the negotiation and preparation phase, but the Czech science diplomat based in Washington has played a key role in facilitating contacts between MU and Georgetown.[25]

In sum, Czech activities in the areas of science diplomacy and cyber security have taken place on a random or ad hoc basis so far, without any overall strategic plan.

Before the Czech Republic deployed its science diplomats and cyber attachés, diplomacy related to cyber issues was governed by the personal interests of individual diplomats, again, without any strategic framework. The first and so far the last effort to establish a formal basis for Czech science diplomacy was that of Pavel Bělobrádek, who became Deputy Prime Minister for Science, Research and Innovation in January 2014. During his almost three years in the office, he initiated the posting of two science diplomats—one to Israel in autumn 2015 and another to the United States in spring 2017. He had planned to

[20] Interview 3, NCISA, Prague, 26 March 2019.
[21] MN CD ET: Project. Retrieved from: https://mncdet.wixsite.com/mncdet-nato as accessed 12 April 2019.
[22] Interview 3, NCISA, Prague, 26 March 2019.; Interview, Masaryk University, Brno, 19 March 2019.
[23] Interview, Masaryk University, Brno, 19 March 2019.
[24] Interview, Masaryk University, Brno, 19 March 2019.
[25] Interview, Masaryk University, Brno, 19 March 2019.

deploy a third such diplomat to the Far East.[26] However, this promising start was derailed when Bělobrádek resigned in December 2017. No other politician continued Bělobrádek's plan to build up a network of science diplomats and formulate a strategic framework for their work in the area. Thus, although there is a clear need for more science diplomats, the Czech Republic continues to have only two of them, whose work lacks clear leadership and sustained political support. The overall situation of Czech science diplomacy continues to be based on unsystematic decision making and the individual interests of diplomats.[27]

The disorder in Czech science diplomacy also influences relations between the two science diplomats and NCISA's cyber attachés, particularly those who are posted to Washington and Tel Aviv. For example, one of the four stated priorities in the work of the science diplomat in Washington is cyber security. Thus, there are two diplomats at the same embassy dealing with the very specific topic of cyber security, which might confuse foreign partners. Moreover, the competencies of the two diplomats have not been clearly defined by their leadership. Instead, their work overlaps and coordination is ad hoc, depending on their individual agreement on the spot to cooperate on particular issues.[28] Although it might be agreed that the science diplomat should have the lead on cooperation with the academic sector in cyber security, sooner or later the cyber attaché will come across new contacts in that domain. It then becomes a question whether it would not be better to create a "thematic" division of work that would put the cyber attaché in charge of science diplomacy for cyber security issues.[29]

Another disharmony in the Czech Republic's science diplomacy is the absence of a common understanding within the government of what science diplomacy actually is. The MFA and other government bodies continue to ask themselves what kind of activities can be considered science diplomacy.[30] If they could definitively answer that question, preferably by producing a strategy for science diplomacy, the government would know better how to approach such issues. Hopefully, science diplomacy would then receive its deserved share of attention and would not be closely so linked to economic diplomacy (as for instance through PROPED missions) as it is.[31]

Similarly, there is a certain level of disagreement about who is suitable to be a science diplomat with a focus on cyber security. The selection of career diplomats with no scientific or academic experience in the field to be the first Czech science diplomats evoked criticism.[32] Some argue that a science diplomat does not need to possess a scientific background. Such a person need only to be a socially skilled manager because what is needed is only a mediator who does not choose the scientific fields to emphasise or determine the content of policy.[33] Others argue that although a science diplomat should be an MFA employee, he or she should have rich experience in the sphere of science, preferably having accomplished academic projects on both the national and international levels. Only that way will a diplomat gain the respect of his partners and be considered a

[26] Government of the Czech Republic: Deputy Prime Minister Bělobrádek Officially Introduced the Second Science Diplomat. Retrieved from: https://www.vyzkum.cz/FrontAktualita.aspx?aktualita=807455 as accessed 12 April 2019.

[27] Interview, CzechInvest, Prague, 29 November 2018.; Interview 1, NCISA, Brno, 17 January 2019.; Interview, Ministry of Foreign Affairs of the Czech Republic, Prague, 5 December 2018.

[28] Interview 3, NCISA, Prague, 26 March 2019.

[29] Interviews 3 & 4, NCISA, Prague, 26 March 2019.

[30] Interview 1, NCISA, Brno, 17 January 2019.; Interview 4, NCISA, Prague, 26 March 2019.; Interview, Masaryk University, Brno, 19 March 2019.; Interview, CzechInvest, Prague, 29 November 2018.

[31] Interview 1, NCISA, Brno, 17 January 2019.

[32] Majer, Vladimír (2017): Science Diplomacy according to Czech Republic. In: Česká pozice. Retrieved from: http://ceskapozice.lidovky.cz/vedecka-diplomacie-po-cesku-dfz-/tema.aspx?c=A170720_232214_pozice-tema_lube ; Interview 1, NCISA, Brno, 17 January 2019.

[33] Interview, Ministry of Foreign Affairs of the Czech Republic, Prague, 5 December 2018.

peer. Such a person does not need to be a career diplomat.[34] Hypothetically, another idea would be to appoint a plenipotentiary science diplomat to focus on cyber security who would not be posted to one country or region but would rather travel the world based on actual need.[35] In contrast to the MFA and its career science diplomats, NCISA has understood the need to send out representatives who are experts in the field they are expected to promote abroad. The NCISA's cyber attachés in Washington, Brussels and Tel Aviv are in fact experts on cyber security who promote the Czech national interest in that domain with clear guidance and express purpose.

The unsystematic nature of science diplomacy in respect of cyber security is also reflected in the various platforms used for communication by diplomats and scientists, which have been developed independently by different stakeholders. The PROPED missions organized by the MFA and CzechInvest's missions abroad have already been mentioned. Another way interested parties can obtain information is the web portals of CzechInvest[36] and NCISA[37]. The former portal is an information gateway which offers a complex overview of Czech research and development to foreign partners and investors. The latter provides details on research and development in the area of protecting classified information and cyber security in the Czech Republic and internationally. However, the portals are rather exceptional. Experts agree that communication and cooperation between Czech diplomats and scientists often occurs on an ad hoc, personalized basis.[38]

Although the state of the art of Czech science diplomacy seems very disorganized, the future of diplomatic efforts in the area of cyber security science appears brighter. At the time of writing this report in spring 2019, NCISA is finishing a document which will define the framework for research in cyber security for the upcoming years. This document, which will probably be published in summer 2019, will, among other things, articulate several areas of interest that should be prioritized by Czech diplomats.[39] Furthermore, NCISA is also planning to organize its own research missions abroad, which would copy the structure of PROPED missions. The intention is to invite Czech research institutions to introduce their work abroad, opening up new opportunities for collaboration with foreign counterparts. This kind of mission will take place two or three times a year, beginning in 2020.[40]

3. Germany's Approach to Science Diplomacy in Cyber Space

3.1 Governance Arrangement and Stakeholders

In the past ten or twelve years, cyber and information security has become an important societal question for Germany, not only an issue for national intelligence agencies. Before, it was seen as a purely governmental topic. Citizens and industries were not understood to be the targets of cyber attack.

[34] Interview 1, NCISA, Brno, 17 January 2019.; Interviews 3 & 4, NCISA, Prague, 26 March 2019.

[35] Interview, CzechInvest, Prague, 29 November 2018.

[36] CzechInvest: Research and Development in the Czech Republic. Retrieved from: http://www.czech-research.com/ as accessed 14 April 2019.

[37] NCISA: Research. Retrieved from: https://nukib.cz/cs/informacni-servis/vyzkum-nukib/ as accessed 14 April 2019.

[38] Interview, CzechInvest, Prague, 29 November 2018.; Interview, Masaryk University, Brno, 19 March 2019.

[39] Interview 3, NCISA, Prague, 26 March 2019.

[40] Interviews 3 & 4, NCISA, Prague, 26 March 2019.

3.1.1. The Institutional Dimension

Now, cyber security is considered a whole-of-government task, which means that different ministries are involved in dealing with it from different angles. Currently, three ministries share cyber security responsibilities:

- Federal Ministry of the Interior
- Federal Ministry of Defence
- Federal Foreign Office

Responsibilities on the governmental level are more or less clearly divided and assigned. The Federal Ministry of the Interior is responsible for the technical means of cyber protection and measures against criminal cyber activities. It is the main body regulating the national architecture of Germany's cyber security activities and procedures. The Federal Ministry of Defence is responsible for cyber defence activities, by which is meant measures against cyber attack, mainly from abroad. The Federal Foreign Office is responsible for foreign policy related to cyber issues and is the main actor for cyber diplomacy. In 2011, the Federal Foreign Office created a special unit, the Cyber Policy Coordination Staff, which works with other ministries and actors to ensure a free, open, secure and stable cyberspace. In its organisational structure there are two main entities dealing with cyber security. The Cyber Foreign Policy and Cyber Security Coordination Staff is the coordinating entity within the Ministry. It deals with all issues of cyber-related foreign policy. In case of an incident or crisis, it creates task forces that include employees of other divisions of the Ministry. In addition, the Foreign Office has a dedicated Director for the United Nations, International Cyberpolicy and Counterterrorism (since 2015 this has been Ambassador Thomas Fitschen).

The Federal Foreign Office has also assigned about 20 cyber attachés to German embassies across the world (including China, Korea, and Israel).[41] The Ministry also has a network of science attachés[42] in 30 embassies around the world (who are not referred to as science diplomats). Some of them are not trained diplomats but are civil servants seconded from the Federal Ministry of Education and Research.[43]

To execute policy in the cyber area, a number of institutions have been created over the years, some with extensive responsibilities:

- The German National Office for Information Security
- The National Cyberdefence Centre
- The German National Cyber Security Council
- The Cyber and Information Domain Service

The German National Office for Information Security, which was founded in 1991, is the national cyber security authority and is linked to the Federal Ministry of the Interior. It shapes security policy for digitalisation through prevention, detection and reaction of incidents for the government, business and society. Its objective is to promote overall IT security in Germany and is the central provider of IT security services to the federal government. It also offers services to the IT industry as well as to other private and commercial IT users and providers.

The German National Cyber Security Council was established in 2011. Its objective is to strengthen cooperation within the government and between the government and the

[41] Interview 3, a representative of German public sector, Bonn/Berlin, 5 April 2019.

[42] In Germany they are called "Wissenschaftsreferenten". The term science diplomat (or in German "Wissenschaftsdiplomat") is not used by the official governmental bodies in this context.

[43] Federal Foreign Office, Außen- und Europapolitik: Internationale Wissenschaftlich-Technologische Zusammenarbeit. Retrieved from: https://www.auswaertiges-amt.de/de/aussenpolitik/themen/aussenwirtschaft/forschungtechnologie/wissenschaftlichtechnologischezusammenarbeit-node as accessed 23 May 2019.

private sector, and to provide recommendations to high officials on strategic issues. The Council falls under the responsibility of the Federal Government's Commissioner for Information Technology. It is comprised of representatives from the Federal Chancellery and State Secretaries from the Foreign Office, the Ministries of the Interior, Defence, Economics and Technology, Justice, Finance, Education and Research, and representatives of the federal Länder (regions).[44] It is thus the most important consultation and exchange forum for cyber security on the national level.

Also in 2011, the National Cyberdefence Centre was established in order to respond to attacks on government computers in Germany. The centre pools the cyber defence resources of many German cyber and intelligence services.[45] It is an advisory body to the German National Cyber Security Council and reports directly to it.

Another new body is the Cyber and Information Domain Service, which is the youngest branch of Germany's military, the Bundeswehr. It is directly responsible to the Federal Ministry of Defence and started operations in 2017. All the competences and capabilities relevant to the cyber and information domains, which were formerly distributed among several Bundeswehr facilities, are located in this new service as of spring 2019.[46] It is the military auxiliary to the National Cyberdefence Centre.

In addition, there are at least two important actors from the private sector that play a key role in national discussions:

- German Telekom
- BITKOM e.V.

German Telekom is the largest telecommunications provider in Europe by revenue and has more than 200,000 employees worldwide (as of 2017).[47] BITKOM is Germany's digital trade association. Founded in 1999, it represents more than 2,600 companies active in the digital economy.[48] German Telekom is a member of BITKOM.

3.1.2. The Link between International Cyber Security Policy and Science

None of the institutions mentioned above are clearly focused on science themselves. However, there are some institutional and operational connections that are worth mentioning. Two governmental bodies already have or are about to institutionalize cooperation with scientific experts.

The Cyber and Information Domain Service already works closely with the University of the Bundeswehr on cyber security-related issues.[49] The University has a research unit on cyber defence and smart data (established in 2013) whose purpose is bringing together researchers, economic actors and government officials. In 2017, a new institute for

[44] The IT Law Wiki, wikia: National Cyber Security Council. Retrieved from: https://itlaw.wikia.org/wiki/National_Cyber_Security_Council as accessed 2 May 2019.
[45] Such as the Federal Office for Information Security, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, the Federal Police, the Customs Criminal Investigation Office, the German Military, the Federal Office of Civil Protection and Disaster Assistance, and the Federal Criminal Police Office.
[46] Cyber and Information Domain Service Headquarters, Press and Information Centre: Cyber and Information Domain. Retrieved from: http://cir.bundeswehr.de/resource/resource/YjR0QzY3aWZvTE4yUHd5Vk55eFhUZFo5dGh3aGZlRTE1VnNvSDFHRnNjUFVxa1l1S3hITWlWRFlRM3ZUSUVjM0NxYXNjck1BVG1RdFBZdWlqNTZ2d3lVY2N0TzRuOE9zakR5STNzcklUTWs9/Flyer_CIR_engl.pdf as accessed 2 May 2019.
[47] Deutsche Telekom: Geschäftsbericht 2017. Mitarbeiterstatistik. Retrieved from: https://www.geschaeftsbericht.telekom.com/site0218/lagebericht/mitarbeiter/mitarbeiterstatistik.html as accessed 2 May 2019.
[48] BITKOM: About. Retrieved from: https://www.bitkom.org/EN/About-us/About-us.html as accessed 2 May 2019.
[49] Interview 2, a representative of German public sector, Bonn, 22 February 2019.

information technology was created by the university.[50] In the near future it intends to fund new professorships.[51] The Service has also worked with some of the Fraunhofer Institutes on a case by case basis.

At the time of this report the Federal Foreign Office is setting up a new research institution, the German Institute for International Cyber Security.[52] The establishment of this institute is mentioned in the national cyber strategy.[53] It will be a virtual institute composed of different German research institutions. Its objectives will be creating scientific output on cyber security issues and providing networking opportunities to domestic and international researchers. It is intended to anticipate trends in cyber security in order to provide up to date, evidence-based advice and guidance for the German government. The institute will be in operation by 2020.

In its new strategy for artificial intelligence, which was just adopted in 2018, the German government announced the creation of a German-French virtual research and innovation network.[54] The strategy does not say whether cyber security will be one of the network's thematic focuses and preparations have not yet moved very far.[55] Given that developments in the field of artificial intelligence will be very interesting to cyber security experts, one can expect that this complex field of research will be one of the key topics for the new network.

The German National Office for Information Security subcontracts research and studies on a case-by-case basis with the aim of providing a knowledge base to decision makers. It has no standing structure or formalized procedures (e.g. working groups) for the Office that organizes cooperation with researchers.[56]

German Telekom interacts with international science from different angles. One example is the Telekom Innovation Laboratories (T-Labs). T-Labs is German Telekom's research and development unit, set up in close partnership with the Technische Universität Berlin. It has sites in Berlin, Darmstadt, Beer Sheva, Budapest and Vienna.[57]

3.1.3. The Strategic Dimension

The Federal Foreign Office is the lead government agency for cyber diplomacy. It uses the term "international cyber policy" to describe its activities.[58] International cyber policy is a cross cutting task impacting virtually all areas of foreign policy. The goal is to ensure that German interests and ideas concerning cyber security are coordinated and pursued in international organizations, such as the United Nations, the OSCE, the Council of Europe, the OECD, and NATO. The priorities for the work of the Federal Foreign Office in those fora include agreement on standards for good governance, the application of international law, and the development of confidence-building measures that enhance international cyber security.[59]

---

[50] Ibid.

[51] Interview 1, a representative of German public sector, Bonn, 9 February 2019.

[52] Interview 3, a representative of German public sector, Bonn/Berlin, 5 April 2019.

[53] Federal Ministry of the Interior (2016): National Cyber Security Strategy for Germany. p.6.

[54] Federal Ministry for Economic Affairs and Energy (2018): Strategie Künstliche Intelligenz der Bundesregierung. p.6.

[55] Interview 4, a representative of German public sector, Bonn/Berlin, 2 April 2019.

[56] Interview 1, a representative of German public sector, Bonn, 9 February 2019.

[57] Deutsche Telekom, T-Labs: Über uns https://laboratories.telekom.com/ as accessed 2 May 2019.

[58] In German "Cyber-Außenpolitik," see also Federal Foreign Office, Foreign and European Policy (2017): International Cyber Policy. Retrieved from: https://www.auswaertiges-amt.de/en/aussenpolitik/themen/cyber-aussenpolitik

[59] Federal Foreign Office, Foreign and European Policy (2017): International Cyber Policy. Retrieved from: https://www.auswaertiges-amt.de/en/aussenpolitik/themen/cyber-aussenpolitik as accessed 23 May 2019.

There are a number of relevant national regulations, strategies and framework documents that relate to cyber diplomacy. The most important are the following:

The German Federal Office for Information Security issues national regulations on protection of cyber security. An Act to Strengthen the Security of Federal Information Technology was passed in 2009 and has been amended regularly since then. The last amendment was in January 2017.[60] It provides a legal framework for all information technology-related issues. Its main focus is on domestic aspects of IT.

A very important document is the German National Cyber Security Strategy, issued in 2016 by the Federal Ministry of the Interior.[61] All government stakeholders were involved in the process of generating that document. The strategy was also notably supported by stakeholders from scientific disciplines, as is stated in the preamble.[62]

That same year, a *White Paper on Security Policy and the Future of the Bundeswehr* was issued by the Federal Ministry of Defence.[63] It underlines Germany's ambition to play an active, substantial role in international security policy and is Germany's key document on its security policy. Cyber security is one of many topics of the white paper. It clearly presents the tasks to be carried out in this context in a specific Cyber Security Strategy.[64]

The Federal Ministry of Education and Research has issued a framework programme on Research for Civil Security from 2018-2023, which provides the main theoretical framework and funding mechanism for all German civil security-related research.[65] Cyber security is mentioned in the Minister's preface to the programme, but is not a specific topic in the body of the paper. It is in fact mentioned as follows: "to ensure that good use is made of the many opportunities and potentials related to digital change. In this context it is important to take account of both the requirements for using digital technologies and applications, and the risks involved".[66] International cooperation is one of the cross-cutting issues of the programme. The Ministry wants to foster international cooperation in civil security research, primarily with Austria, France, India, Israel and the United States.[67]

In summary, the term cyber diplomacy has not been clearly defined by a strategy of any kind that has so far been published in Germany. It is not mentioned under the umbrella of science diplomacy either. The term the government uses, "international cyber policy," suggests that the many actions that might be categorized under that concept are simply considered to be one part of Germany's general diplomatic efforts.

3.2. Governance Practice

Government practice is diverse and is executed by different governmental bodies. Depending on the content and thematic focus of the issue at hand, actors meet in variable geometries.

---

[60] German National Office for Information Security, BSI: Act to Strengthen the Security of Federal Information Technology. Retrieved from: https://www.bsi.bund.de/EN/TheBSI/BSIAct/bsiact_node.html as accessed 2 May 2019.

[61] Federal Ministry of the Interior (2016): National Cyber Security Strategy for Germany.

[62] Ibid, p.17.

[63] Federal Ministry of Defence (2016): The White Paper on Security Policy and the Future of the Bundeswehr.

[64] Ibid, p.38.

[65] This framework programme is a follow-up of the initial framework programme Research for Civil Security from 2012-2017.

[66] Federal Ministry of Education and Research (2018): Research for Civil Security 2018–2023 – A Federal Government Framework Programme. p.4.

[67] BMBF issued joint funding programmes with Austria, France, India, Israel and signed a bilateral agreement with the US Department of State to promote science and technology cooperation on Homeland/Civil Security Matters.

For example, since 2013, Germany has been an active Partner in the Freedom Online Coalition (FOC), a partnership of 30 governments working to advance Internet freedom, and has provided it with financial support. The Federal Foreign Office also plays an active role in the FOC's core group, the Friends of the Chair.

The Ministry of Foreign Affairs has recently established bilateral cyber dialogues with quite a number of countries, among them Brazil, Canada, India, Israel, Japan, Russia, South Korea, and the United States. In May 2017, Germany and Singapore signed a Joint Declaration on strengthening their cyber security cooperation.[68] The declaration promotes cyber security cooperation in key areas, including regular information exchanges, joint training and research programs, and sharing best practices to promote innovation in cyber security. All cyber-related dialogues with EU Member States take place in the Horizontal Working Party on Cyber Issues that was established by the EU in 2016.[69]

European and international cooperation is also a key part of the Research for Civil Security framework programme of the Federal Ministry of Education and Research. Parallel to expanded research collaboration on the European level, the Ministry has set up bilateral funding mechanisms for research with France and Israel. Austria, India and the US are also close partners for cooperation in the field. All these cooperation schemes are based on bilateral agreements.[70]

In the area of cyber defence[71], Germany adheres strictly to the framework of EU and NATO procedures, which are highly formalized. The Federal Ministry of Foreign Affairs has primary responsibility, but the Cyber and Information Domain Service of the Bundeswehr is also deeply involved.

In the area of cyber security, Germany seeks to form coalitions with countries and regions that are like-minded as regards democratic values.[72] It is an obvious pattern and was confirmed in three of the five interviews we conducted.[73] This applies in multinational fora like EU and NATO and also extends to the practice of building bilateral ties. France, Israel and India are examples of states with which Germany has created cyber dialogues. Some bilateral research schemes have also been put into place.

All our interviews hinted that Germany's practices are being formalized, especially those of the Federal Ministry of Foreign Affairs and the Bundeswehr. Official consultations among the responsible ministries are the main instruments of exchange in the cyber security sphere. Intergovernmental consultations take place only among ministries; subordinate agencies are not usually involved, although they can be in particular cases. Power

[68] Cyber Security Agency of Singapore: Singapore Signs Joint Declaration of Intent on Cybersecurity Cooperation with Germany. Retrieved from: https://www.csa.gov.sg/news/press-releases/singapore-signs-joint-declaration-of-intent-on-cybersecurity-cooperation-with-germany as accessed 2 May 2019. Germany has also other bilateral declarations on cyber security, e.g. with Israel and India. The one with Singapore is the most recent one.

[69] European Council, Preparatory Bodies: Horizontal Working Party on Cyber Issues (HWP). Retrieved from: https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-cyber-issues/ as accessed 2 May 2019.

[70] Federal Ministry of Education and Research, Sicherheitsforschung: Bilateral Cooperation in Civil Security Research. Retrieved from: https://www.sifo.de/en/bilateral-cooperation-in-civil-security-research-2219.html as accessed 23 May 2019.

[71] In the German context term cyber defence describes mostly measures taken against cyber attacks mainly from abroad, while cyber security is used as a general term that subsumes cyber protection, cyber defence, cyber security policy and cyber foreign policy (Federal Ministry of Defence (2016): The White Paper on Security Policy and the Future of the Bundeswehr. p.38).

[72] This was expressed independently by different interviewees: Interview 1, a representative of German public sector, Bonn, 9 February 2019.; Interview 3, a representative of German public sector, Bonn/Berlin, 5 April 2019.; Interview 5, a representative of the German private sector, Bonn, 1 February 2019.

[73] Interview 2, a representative of German public sector, Bonn, 22 February 2019.; Interview 3, a representative of German public sector, Bonn/Berlin, 5 April 2019.; Interview 5, a representative of the German private sector, 1 February 2019.

relationships are very clear and are organized from the top down. All the officials we interviewed stated that cooperation is quite good, fruitful, and driven by content. Disagreements are handled in a formal manner.

3.2.1. On the Limits of Science Cyber Diplomacy

Germany has no overall strategic approach that links science, cyber security and science diplomacy. There are institutionalized connections between some institutions of cyber security or cyber defence and scientific institutions (as there are between the University of the Bundeswehr and the Cyber and Information Domain Service). In general, government institutions have addressed scientific issues on a case-by-case basis. This might change when the new German Institute for International Cyber Security begins to operate. Its main purpose will be to inform the government about future trends.

Because Germany has assigned quite a large number of cyber diplomats and science diplomats to its embassies around the world, one might think that cooperation between colleagues working in the two fields would be natural, since both types of diplomats work in the same embassy. An interview with a representative of the public sector suggests the opposite: the science and cyber attachés usually stick to their clearly defined responsibilities and there are no formal schemes for cooperation or interfaces between the two positions.[74] For instance, the science attaché in Tel Aviv does not participate in the bilateral cyber dialogue between Germany and Israel. The same is true for most of Germany's other bilateral cyber dialogues. Who participates depends on the people in charge and the degree to which they are interested in linking both spheres of diplomatic activity.

All our interviews showed that the concept of science diplomacy is not well understood in the cyber security world. All the interviewees were very interested in it, however. They said there would be added value in learning more about it as a first step toward exploiting its merits for improving cyber security. As there are no formalised structures for exchanges between science diplomats and cyber diplomats, even within the Ministry of Foreign Affairs, there is clearly room for a more formalized, strategic approach to linking the two "worlds" in the future.

Because the Ministry of Foreign Affairs and the Federal Ministry of Education and Research have only recently started to develop the concept of science diplomacy, which remains at a very general level, it will be interesting to see whether they continue down that path and how they organise and formalise their science diplomacy efforts.

4. France's Approach to Science Diplomacy in Cyber Space

4.1 Governance Arrangement

Since about 2010, technological changes (cloud computing, big data, artificial intelligence, etc.), rising awareness of the vulnerability of computer systems, and the technological gap between the United States and Europe revealed by the Snowden case have boosted investment in cyber security. The challenges now cut across fields in information technology, involving companies, universities, laboratories, governmental agencies, and interdepartmental government services. All of those actors have contributed to development of an official French document that addresses cyber strategy, cyber defence, and cyber diplomacy. In 2015, digital security became an express national priority. In 2017, France adopted an international digital strategy, which encompasses cyber security

[74] Interview 3, a representative of the public sector, Bonn/Berlin, 5 April 2019.

policies. First conceived mainly as a technical issue, cyber security has become more of a diplomatic issue for governments and policymakers.

The French cyber doctrine milestones (listed with French acronyms of the agencies that have produced them) are:

- SGDSN, Livre Blanc sur la Défense et la Sécurité Nationale (2008)
- ANSSI, Défense et sécurité des systèmes d'information - Stratégie de la France (2011)
- SGDSN, Livre Blanc sur la Défense et la Sécurité Nationale (2013)
- ANSSI, Stratégie Nationale pour la sécurité du numérique (2015)
- Ministère des Armées, Revue stratégique de défense et de sécurité nationale (2017)
- MEAE, Stratégie internationale de la France pour le numérique (2017)
- SGDSN, Revue stratégique de Cyberdéfense (2018)

The lead government agency responsible for cyber security issues is the French National Cybersecurity Agency (ANSSI), attached to the General Secretariat for Defence and National Security (SGDSN), which reports directly to the Prime Minister. Created in 2009, ANSSI employs over 500 people and provides expertise and assistance to government departments and other institutions, and for international negotiations.

The Ministry of Home Affairs' mandate is defending against all kinds of cyber criminality, whether it targets government agencies, businesses, or private individuals. The Ministry of the Armed Forces (MinArm) has two concerns: protecting its own computer networks from attack and integrating digital combat into military operations. In addition to the Weapons Directorate (DGA) and the International and Strategic Affairs Directorate (DGRIS), the Ministry of the Armed Forces created a military command (COMCYBER) in 2017 tasked with developing a cyber defence strategy.

The Ministry for European and Foreign Affairs (MEAE) coordinates cyber diplomacy and acts as France's representative to the United Nations Groups of Governmental Experts (GGE), where international rules for behaviour in cyber space are discussed. Its representatives, together with those of the other authorities with competencies in cyber security (MinArm and ANSSI), are implementing the Cyber Defence Pledge adopted by NATO in June 2016. They are also promoting adoption of standards for responsible behaviour in cyber space, and are taking action within the OSCE to implement confidence-building measures.[75]

Until 2017, the MEAE devoted only half of one of its posts to cyber issues: it now has assigned two full-time equivalent employees to the Strategic Affairs Directorate, plus a cyber counsellor in the French Permanent Representation in Brussels. Last but not least, France named a digital ambassador in 2017, who is attached to the MEAE. He has gradually expanded his portfolio (data policy, electronic proof, etc.). The ambassador participates in international negotiations in NATO and was notably involved in the preparation of the Paris Call for Action in November 2018.

The importance of cyber security issues increases the usefulness of several scientific disciplines in creating policy tools and attracts scientists from various disciplines to government services. Computer sciences, cryptography, international law, political sciences or geo-strategy have all had an impact on political decisions and are valued for that. The Director General of ANSSI has said that "cybersecurity is a fascinating and highly scientific field spanning a range of disciplines and involving a wealth of organisations and actors, from both the public sector and the business world, within France and internationally".[76] The MEAE's international digital strategy paper stresses that it must:

[75] MEAE: La France et la cybersécurité. Updated May 2019. Retrieved from: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-et-securite/cybersecurite/

[76] ANSSI: A Word from the Director General. Retrieved from: https://www.ssi.gouv.fr/en/mission/word-from-director-general/

…contribute to the development of French strategic thinking on cybersecurity issues. It seems imperative to continue to acquire, particularly at the national level, skills and knowledge in terms of foresight, research and multidisciplinary expertise…. It is important that the MEAE continues to promote specialized, interdisciplinary centres of excellence that capture the major transformations (not only in the security field) in the digital age. The MEAE is also committed to cooperating with leading French think tanks and research groups to help them develop real expertise on these topics.[77]

The sciences are strongly connected to policy areas. The increasing importance of cyber issues has contributed to development of a complex framework associating different types of actors in both government administration and academia.

4.2 Stakeholders and Governance Practice

Broadly speaking, France has four strategies for making science-related policies. The first is internalising scientific expertise. ANSSI has its own in-house science department, which consists of five laboratories, mainly in the computer sciences field. Most of its senior officers are engineers or hold a PhD in computer science. Employees of its five laboratories are working on doctoral theses. MinArm's DGA and DGRIS provide funding for PhD researchers in the hard sciences and in strategic analysis. The Ministry has its own research department. It also created the Military School Institute for Strategic Research (IRSEM) in 2010. As well as conducting their own scientific research, its members regularly submit prospective strategic studies to the Ministry. Founded in 1973, the Centre for Analysis, Forecasting and Strategy (CAPS) is an advisory body for the MEAE.[78] IRSEM and CAPS have cyber divisions staffed with their own researchers. One researcher from CAPS is dedicated solely to providing the MEAE and France's digital ambassador with expertise.

The second strategy is outsourcing. Historically, the French ministries have had their own privileged advisory channels. The MEAE, for example, regularly consults with experts from three think tanks: the French Institute for International Relations (IFRI), the Institute for International and Strategic Affairs (IRIS), and the Foundation for Strategic Research (FRS), all of which are dedicated to studying geopolitical and strategic issues and regularly publish studies of cyber issues. Furthermore, the Ministry of the Armed Forces subcontracts studies to researchers in the framework of a three-year renewable contract. CEIS is an important think tank that is very active with regard to strategic analysis. It is one of the main contractors with the French government and has a team of 15-20 in-house experts along with support from outside academic researchers.

A third, similar strategy is partnership. It is hard to describe the entire range of more or less formalized collaborations among scientific institutions (like the French National Research Institute for the Digital Sciences (INRIA)), individuals, and political decision-makers. One of ANSSI's current objectives is strengthening its links with academia. ANSSI created a Scientific Council in 2018 to facilitate its scientific cooperation with external researchers. In addition to several partnerships with research centres, ANSSI also participates in international scientific initiatives — for example, through the EU's Strategic Programs for Advanced Research and Technology in Europe (SPARTA) competence network.[79] ANSSI organises special events at French embassies abroad as part of its

[77] MEAE (2017): Stratégie internationale de la France pour le numérique. p. 30, Retrieved from: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/strategie-internationale-de-la-france-pour-le-numerique/

[78] From that point of view, science in diplomacy is traditionally ingrained in French foreign policy.

[79] See the EU part of the cyber security report for more details.

program of cooperation with foreign countries. These dialogues involve Embassy representatives and cyber scientists from their host countries.[80]

The fourth strategy involves ad hoc interfaces between government and experts. Emerging challenges related to cyber issues have actually redesigned the playing field and have promoted the creation of common spaces that gather together different types of actors. Two initiatives were often mentioned during our interviews. The Castex Chair was created in 2010 as a research institution specialising in the analysis of the geopolitics of cyber space, and is closely linked to both MinArm and the MEAE. The Castex Chair does not claim to "influence" but rather to "enlighten" decision makers, by organising seminars that bring together experts, academics, business actors and civil servants. The AMNECYS project (for Alpine Multidisciplinary NEtwork on CYber-security Studies) also brings together scientists from different fields and laboratories and in-house researchers who are engaged in various policy and diplomatic arenas.

Turning now to two specific sets of activities, we can make the links between science and diplomacy in France clearer. The first set is the activities of the French National Research Institute for the Digital Sciences (INRIA), which involve both science for diplomacy and diplomacy for science. INRIA is one of the main French research centres involved in cyber issues. It underwrites 25% of France's academic research in the area of cyber security and has 200 full-time employees working on that priority.[81] Together with other research teams, INRIA takes part in several bilateral projects of cooperation, particularly with Germany and Japan.

INRIA actively supports Franco-German bilateral cooperation on cyber issues. As a matter of fact, cyber security is one of the fields covered by the Sixth Forum on Franco-German Research Cooperation. A strategic initiative to establish a joint Cybersecurity Roadmap was approved by both countries' Ministers for Research in June 2018 with the goal of promoting synergy between France and Germany. According to the German Ministry, "[c]ooperation in cybersecurity can serve to study and test key enabling technologies in the field of digital sovereignty and to apply these technologies in association with industrial partners in both countries".[82] Prepared under the aegis of INRIA and Fraunhofer AISEC/TU, the scientific roadmap encompasses topics and instruments that include research events and projects, new facilities, support for scholars' international mobility, and joint education.

The second set of activities is INRIA's participation in collaboration between France and Japan on cyber security research, which has been ongoing since 2015. Annual workshops gather together researchers from both countries. They take advantage of "each country's specificities and excellence in the domain and a shared vision of geo-strategy and privacy concerns".[83] The workshops receive financial support from the French embassy in Japan. Interestingly, the embassy counsellors are given a chance to voice their opinions on the topics under discussion. The researchers focus on industrial and political issues (the spread of disinformation, development of 5G services, etc.). As one interviewee noted: "we also use the academic dimension in order to tackle other, political, issues".[84] In that sense, the French-Japanese initiative is not only about international scientific cooperation (diplomacy for science) but also about sharing a common understanding of political issues (science for diplomacy).

[80] See, for example, the partnership between France and Japan on cyber security research, involving INRIA researchers (INRIA: Joint collaboration between France and Japan on Cybersecurity Research. Retrieved from: https://project.inria.fr/FranceJapanICST/)

[81] INRIA (2019): Cybersecurity. Current challenges and Inria's research directions. White Book 3.

[82] Federal Ministry of Education and Research (2018): Cybersecurity Research – Proposal to develop the synergy between France and Germany. Position paper by the expert group.

[83] INRIA: Joint collaboration between France and Japan on Cybersecurity Research. Updated March 2019. Retrieved from: https://project.inria.fr/FranceJapanICST/

[84] Interview, INRIA, 6 February 2019.

Another interesting initiative is related to science in diplomacy. Inaugurated in 2011, attached to the Institute of Higher Defence Studies, the Castex Chair for Cyber Strategy "aims to develop fundamental and applied research in the geopolitics of cyberspace in order to feed strategic reflections related to its political, economic, military and regulatory importance".[85] For several years, the Castex chair has organized conferences and workshops bringing together young researchers, experts in the cyber field, entrepreneurs, military figures, civil servants, and politicians to deal with geopolitical, strategic, legal, and sovereignty issues in cyber space. The Castex Chair facilitates formal and informal debates involving both government officials and entrepreneurs.[86] It has also produced several significant results. The Post-Soviet Cyberspace Observatory and the Arabic-speaking Cyberspace Observatory are two examples. Staffed by two teams of researchers, the Observatories are connected to the Directorate General for International Relations and Strategy. They have regular contacts with COMCYBER, a unit of the Ministry of the Armed Forces.

Interestingly, the chairwoman of the Castex Chair has been given some diplomatic positions: she is a board member of the *Defence and National Security Strategic Review* published by MinArm[87] and is directly involved in the Paris Call for Action of 2018. She is often consulted by MEAE diplomats as they prepare for international negotiations in NATO. Her contribution is in identifying and framing salient issues, interpreting global trends, producing technical proposals, and organising global events and meetings.[88] The Castex Chair is a good example of science diplomacy in action.

Beyond those examples, a range of general observations can be made about France's cyber security infrastructure. In a country where high civil servants have traditionally had minimal interaction with scientists, science diplomacy reflects that cyber security is an emerging issue of global importance, which requires new skills that not all administrators have. Specific knowledge — and not only technical knowledge, such as computer skills — complements the traditional expertise of government employees. For example, one diplomat explained to us how valuable experts in international public law have been to understanding and construing the evolution of the cyber-doctrines of foreign countries.[89] By combining different research approaches and fields of study, researchers produce original information (such as the cartography of cyber space) which can then be converted into valuable advice for diplomats and policy makers.

Researchers adapt their language, their way of working, and also their publications to produce useful policy briefs for officials. One source from the MEAE mentioned to us: "we do not have time enough to read fifty pages, we only read two-page papers".[90] It is remarkable that some scientists we interviewed spontaneously used the traditional language of diplomacy: some of them told us about the "1.5 track meetings" in which they had participated.[91] All that indicates that researchers are taking an active part in science diplomacy. The common social background of the researchers and diplomats — they are often young, with similar kind of education, and many of them are reserve officers or grew

[85] Chaire Castex de Cyberstrategie: The Aims of the Castex Chair. Retrieved from: http://www.cyberstrategie.org/?q=en/the-aims-of-the-castex-chair

[86] See for example the international conference organized at UNESCO in April 2017. ANSSI (2017): Conférence "Construire la paix et la sécurité internationals de la société numérique". Retrieved from: https://www.ssi.gouv.fr/actualite/conference-construire-la-paix-et-la-securite-internationales-de-la-societe-numerique-le-programme-maintenant-disponible/

[87] The review is the official document whose purpose is to set up a strategic framework for the French defence effort. Ministry of the Armed Forces (2017): Defence and National Security Strategic Review.

[88] Interview, Castex Chair, 23 April 2019.

[89] Interview, MEAE, 9 April 2019.

[90] Ibid.

[91] Usually, track 1 is an official one. Track 1.5 can (but not necessarily) be official and involves government staff as well as external experts, while track 2 does not involve the government at all.

up in military families — facilitate cooperation between the fields. But, above all, their interaction contributes to the institutionalisation of a "common language",[92] shared agendas, and similar ways of working.

Nevertheless, "cyber science diplomacy" does not seem to exist as a specific sub-discipline in the French context, or at least it is not well recognized as such. It does not appear in any text, and there is no clear statement of the way the sciences and cyber diplomacy can cooperate. Cyber security is not mentioned in the MEAE's 2013 science diplomacy report,[93] nor has it appeared since then in the MEAE's agenda for science diplomacy.[94]

One of the explanations for this is that the framework of "cyber" diplomacy is quite fragile in France. The Digital Ambassador's portfolio grew quickly and he lacks resources (having only two full-time staff), which weakens his interactions with academics. According to a diplomat in charge of cyber security at the MEAE, the attention that French embassies devote to cyber issues "depends on the people in charge and on the role configuration".[95] Embassies' interest in cyber issues does not exceed the personal interest of their ambassadors. For example, a diplomat told us that cyber issues are mainly a strategic affairs issue for embassies[96], and an academic explained that his main interlocutor at the French embassy in Japan was the scientific advisor for information and communications technologies[97]. Most of the time, cyber issues are not formally reflected in the embassies' organizational charts.[98]

Moreover, relationships between diplomats and scientists remain rather narrow and involve only a very few actors (maybe a dozen, at least as far as the "social sciences" are concerned). Cooperation depends a lot on the personal relationships that stakeholders maintain. Even where those personal relationships exist, they generally are informal, and they are not everywhere institutionalised. Academics do not receive much feedback on their work from the diplomats. They often say that diplomats still need to develop a better understanding of cyber issues and their importance to the nation. In short, cyber science diplomacy in France needs stronger institutional support.

5. European Union's Approach to Science Diplomacy in Cyber Space

5.1 Governance Arrangement

The first milestone in the EU's development of diplomacy in cyber space was the adoption of a grand strategic document: the *Cybersecurity Strategy of the European Union — An Open, Safe and Secure Cyberspace*. The strategy was adopted in February 2013 by the European Commission, together with the High Representative for Foreign Affairs and Security Policy. It presented the EU's vision for responding to various cyber threats and safeguarding European cyber space. It set five priorities: building cyber resilience, reducing cyber crime, developing cyber defence capabilities and the industrial and technological

[92] Interview, Castex Chair, 5 February 2019.

[93] MEAE - Direction générale de la mondialisation, du développement et des partenariats (2013): Une diplomatie scientifique pour la France. January 2013. Retrieved from: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/

[94] MEAE: Scientific Diplomacy. Retrieved from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/scientific-diplomacy/

[95] Interview, MEAE, 9 April 2019.

[96] Interview, French Permanent Representation, 24 April 2019.

[97] Interview, INRIA, 6 February 2019.

[98] See for example the embassy of France in Japan: Embassy of France in Tokyo: Présentation des services. Retrieved from: https://jp.ambafrance.org/Presentation-des-services#Service-pour-la-science-et-la-technologie

resources for cyber security and, finally, promoting core EU values.[99] The strategy also set the further goal of articulating "a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector".[100] Thus, the desire to mainstream cyber security issues into EU international relations and the Common Foreign and Security Policy (CFSP) gave birth to EU cyber diplomacy.

Pursuant to the 2013 *Cyber Security Strategy*, the Commission tabled a package of cyber security measures in September 2017. The package introduced new initiatives to further develop European cyber response and resilience — among others, strengthening the role and mandate of the EU Agency for Network and Information Security (ENISA), introducing a cyber security certification scheme recognised across the EU Member States, and prompt implementation of the Directive on Security of Network and Information Systems (the NIS Directive). The package does not ignore the EU's external relations; it promotes the application of international law in cyber space, responsible state behaviour, and the development of bilateral cyber dialogues.[101]

Cyber security has become a top diplomatic issue for the EU. The 2015 Council Conclusions on Cyber Diplomacy proposed a range of specific objectives and principles for preventing conflict, reducing threats to cyber security, and increasing stability in international relations as regards cyber space.[102] The EU Cyber Diplomacy Toolbox was adopted by the EU in September 2017. It completes a triad of important EU cyber diplomacy documents. The toolbox's purpose is to encourage greater cooperation and more agile joint EU diplomatic reaction to malicious cyber events. It articulates possible countermeasures, including sanctions, that could be taken by the CFSP to respond to cyber attacks originating beyond Europe's borders.

Although these strategic documents laid the foundation for EU cyber diplomacy and its future development, none of them addresses the use of science as a diplomatic tool for enhancing cyber cooperation with external actors. On the other hand, although it appears that the EU has not formulated a coherent science diplomacy strategy for cyber space on paper, in practice it has been active in the field to a certain degree.

5.2 Stakeholders and Governance Practice

When it comes to cyber diplomacy on a general level, the European External Action Service (EEAS) department specialized in cyber issues has progressively developed in recent years. As of spring 2019, it employs six people. It is interesting to note here that Heli Tiirmaa-Klaar, the former Head of Cyber Policy Coordination for the EEAS from 2012 to 2018, was herself a cyber expert (she earlier coordinated the implementation of the Estonian cyber strategy). Her successor, Wiktor Staniecki, is a career diplomat with a traditional background. This change could mean that cyber issues are increasingly a routine part of the diplomatic agenda. The EEAS cyber department is in charge of advocacy at NATO and the OSCE. It notably promotes the EU strategy for preventing conflicts and provides support to Member States that have not developed their own capacities and policies in the

[99] European Commission (2013): Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[100] Ibid.

[101] European Commission: Cybersecurity. Retrieved from: https://ec.europa.eu/digital-single-market/en/cyber-security

[102] European Council and Council of the EU (19 June 2017): Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanction. Retrieved from: https://www.consilium.europa.eu/fr/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

field.[103] The EEAS is also active in bilateral cyber dialogues between the EU and third countries and participates in both international conferences and more informal relationships.

International scientific cooperation is important to preserving the EU's "strategic autonomy", which is one of its top priorities. Indeed, under the influence of some Member States (France and Germany in particular), the EU institutions have taken action over several years to ensure the EU's technical sovereignty and enhance its cyber resilience. The EU's strategy rests on three pillars: legislation (the NIS Directive), normative leverage (appealing to standards and norms to encourage consensus), and industrial tools (such as public-private partnerships).[104] Synergy with the scientific community is a cross-cutting objective and is a tool used internally for developing and facilitating innovative projects. The EU has several sources of funding for such projects. The Directorate General for Migration and Home Affairs (DG Home) and especially the Directorate General for Communications Networks, Content and Technology (DG CNECT) have their own budget lines to finance technical projects. The main funding instrument is the Horizon 2020 (H2020) work programme 2018-2020 "Secure Societies - Protecting Freedom and Security of Europe and its Citizens". In 2018, seven H2020 projects in the cyber security field were funded under the rubric of innovation actions, five under research and innovation actions, two under the Marie Skłodowska-Curie actions, one under Coordination and Support Actions, and one by the European Research Council. The largest number of projects was funded under the Small and Medium Enterprise funding scheme (11 projects).[105]

The European Commission's proposal for a European Cybersecurity Competence Network and Centre also supports some of the current projects. The main purpose of this new initiative, which is funded under the next multi-annual financial framework for 2021 to 2027, is to "help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market" while increasing "the competitiveness of the EU's cybersecurity industry and turn[ing] cybersecurity into a competitive advantage of other European industries".[106] The Centre, together with the Network, is supposed to clarify the EU funding landscape by implementing a coordinating mechanism for cyber security-related financial support from the Horizon Europe and Digital Europe programmes.[107] It helps to promote a "European cybersecurity community" in that way.[108]

At the time of writing this report, 63.5 million euros are invested in four Horizon 2020 pilot projects dealing with electronic government and the economic dimensions (energy, finance, transport) and technological dimensions (ICTs, industry) of cyber security.[109] The cyber security programme Competence Research Innovation (CONCORDIA) gathers 46

[103] Interview, EEAS, 24 April 2019.

[104] European Commission press release (5 July 2016): Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats. Retrieved from: http://europa.eu/rapid/press-release_IP-16-2321_en.htm

[105] Amires: Cybersecurity Projects within H2020. Retrieved from: http://amires.eu/cyber-security-projects-within-h2020/

[106] European Commission: Proposal for a European Cybersecurity Competence Network and Centre. Retrieved from: https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

[107] Council of the EU, press release (2019): EU to pool and network its cybersecurity expertise – Council agrees its position on cybersecurity centres. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/
The major binding criterion was to bring together at least twenty partners from at least nine countries to work on four use cases.

[108] Interview, a SPARTA member, 6 February 2019.

[109] European Commission: Cybersecurity: Horizon 2020 Pilot Projects. Retrieved from: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57561

partners involving 14 member states; Cyber Security for Europe (CSE) gathers 43 partners involving 20 member states; ECHO gathers 30 partners involving 15 member states; and, finally, SPARTA gathers 44 partners involving 14 member states. The SPARTA consortium links national agencies (like ANSSI in France), laboratories, and industrial actors such as Thales. Its purpose is to innovate defence against new cyber attacks, to ensure protection of highly connected computing environments, and promote the security of artificial intelligence.

Although these initiatives are all focused on the Member States and stakeholders within the borders of the EU, one of the four pilot projects announced at the beginning of 2019 seeks to have an impact beyond the EU. The European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) project includes 30 partner organizations from 15 EU Member States and Ukraine. It aims to "organize and optimize the currently fragmented cybersecurity efforts across the EU".[110] The question remains, will these ambitious plans stay only on paper or will they be carried out in practice?

Bilateral cooperation with third countries has been one of the objectives of the EU's funding policies for the past several years. As stated in one of the EU's calls for action:

an exchange of views and possible cooperation around cybersecurity and privacy research and innovation approaches, policies and best practices with like-minded third countries is necessary in order to bring relevant elements of comparison and allow European stakeholders (public and private) to actively participate in those discussions which will determine the future global cyber security landscape.[111]

The EU first introduced this particular type of diplomacy by funding wide-ranging projects of other countries. It frequently uses this tool in its relations with its strategic partners, but what follows below shows that it is also a useful tool of cooperation with other countries.

Earlier, the EU's Seventh Framework Programme (FP7) of 2007–2013 funded several ICT-oriented projects that led to the development of the EU's science diplomacy in cyber topics. To name one of them, the Facilitate Industry and Research in Europe (FIRE) project operated between 2012 and 2014. FIRE's goal was to "provide a strategic approach, organizational support and network capability for researchers, technology developers, consultants, system integrators and governments to improve their European co-operation". It also sought to "find alignment and collaborative or export opportunities for European technology solutions with other targeted markets such as the US, Canada, Brazil, Argentina, Chile and Japan".[112] Another FP7 ICT project was Building International Cooperation for Trustworthy ICT (BIC), which ran between 2011 and 2013. The project was aimed at developing models for cooperation between EU researchers and their colleagues in Brazil, India and South Africa, countries which "represent significant emergent world-impacting information economies through the scale and sophistication of their growing ICT sectors".[113] The BIC project offered added value in two other ways. It extended cooperation to include stakeholders involved in another, previously established project, INCO-TRUST, namely the USA, Japan, Australia, South Korea and Canada.

[110] ECHO (25 February 2019): ECHO Project Press Release. Retrieved from: https://www.echonetwork.eu/wp-content/uploads/2019/02/Echo_press_relase_2502.pdf

[111] European Commission (14 October 2015): EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/ds-05-2016

[112] European Commission – Cordis: FIRE – Objective. Retrieved from: https://cordis.europa.eu/project/rcn/105736/factsheet/en

[113] European Commission – Cordis: BIC – Objective. Retrieved from: https://cordis.europa.eu/project/rcn/95486/factsheet/en

Furthermore, BIC promised to sustain development of its activities even after its official end date by means of its International Advisory Group and Working Group structures.[114]

Besides the tool of funding projects, the EU develops strategic partnerships with key state players around the globe[115] that include cooperation on cyber security issues. The types of cyber cooperation with the EU's strategic partners vary based on the character of the partners' relationships with the EU outside of cyber space. For example, while the EU's cyber cooperation with the United States is the most active, mirroring its generally good bilateral relations with the U.S., its activities with the Russian Federation are focused mainly on confidence-building measures because Russian territory is perceived to be the source of numerous cyber attacks and cyber espionage against the EU.[116]

The EU's strategic cyber partnerships with Japan and the United States are its most highly developed. In 2010, the EU and the U.S. established a Working Group on Cyber-security and Cyber-crime, whose main goal has been addressing priorities related to cyber security and cyber crime.[117] Another important platform for bilateral cyber relations is EU-U.S. Cyber Dialogue, which held its first meeting in December 2014 and has continued to meet annually. The dialogue is co-chaired by representatives from the U.S. Department of State and the EEAS. It serves as an official platform for information-sharing and coordination of actions on cyber-related issues. Similarly, the EU and Japan have organized annual Cyber Dialogue meetings since 2014, as a platform for regular cooperation. The goals are similar to those of the EU-U.S. Cyber Dialogues. The dialogues affirm a commitment to closer cooperation and to improving the existing bilateral structures and practices.[118]

Because the strategic cyber partnerships with Japan and the United States are the EU's most highly developed, they include elements of cyber science diplomacy. The EU-U.S. Cyber Dialogue in December 2016 is an example. During its third meeting, the EU and U.S. representatives announced the creation of the Transatlantic Cyber Policy Research Initiative (TCPRI). The press release for the event notes that:

[In order to] support burgeoning governmental transatlantic cooperation in cyberspace, the European Union and the United States launched the Transatlantic Cyber Policy Research Initiative, bringing together European and U.S. civil society, academic, industry and think-tank experts to address key cyber policy challenges and increase policy research capacity on cyber issues.[119]

Although the TCPRI initially appeared to be the most promising initiative in EU-U.S. cyber relations, both partners failed to deliver on their plans to take appropriate, timely action. That prompted a German independent think-tank, the Stiftung Neue Verantwortung (SNV), to hold a workshop that aimed to discuss the future of the TCPRI. The workshop convened sixteen cyber security experts and researchers from both the United States and the EU in Washington, D.C. in December 2018 to devise a new model for implementation of the TCPRI.[120]

---

[114] European Commission – Cordis: BIC – Objective. Retrieved from: https://cordis.europa.eu/project/rcn/95486/factsheet/en ; BIC: Home. Retrieved from: http://www.bic-trust.eu/index.html

[115] These are the USA, Canada, Japan, Brazil, Russia, China, India, Mexico, South Africa and South Korea.

[116] Renard, Thomas (2018): EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. In: *European Politics and Society. 19*(3), pp. 321-337.

[117] Council of the EU (20 November 2010): EU-US Summit, joint statement. Retrieved from: http://europa.eu/rapid/press-release_PRES-10-315_en.htm?locale=en

[118] EEAS, press release (14 March 2018): 3rd EU-Japan Cyber Dialogue – Joint Elements. Retrieved from: https://eeas.europa.eu/topics/eu-international-cyberspace-policy/41330/3rd-eu-%E2%80%93-japan-cyber-dialogue-joint-elements_en

[119] EEAS, press release (16 December 2016): EU-US Cyber Dialogue. Retrieved from: https://eeas.europa.eu/headquarters/headquarters-homepage_en/18132/EU-U.S.%20Cyber%20Dialogue

[120] SNV (2018): EU-US Cyber Diplomacy Workshop on Transatlantic Cyber Policy Research Initiative. Retrieved from: https://www.stiftung-nv.de/en/node/2484

Another promising initiative in EU-U.S. cyber relations that gives hints of the development of cyber science diplomacy is the Accelerating EU-U.S. Dialogue for Research and Innovation in Cybersecurity & Privacy (AEGIS). The AEGIS project, funded under Horizon 2020 and begun in 2017, aims, among other things, "to promote collaboration and innovation partnerships between researchers, innovators, and industry from Europe and the US with the goal of coordinating the multiple research efforts underway in the areas of cybersecurity and privacy".[121] Besides publishing white papers, policy briefs and recommendations on relevant topics, AEGIS also holds two regular events, a Cybersecurity Reflection Group Round Table and the Open Cyber Camp EU-U.S. The Cybersecurity Reflection Group Round Tables gather EU and U.S. experts, policy makers, researchers and business leaders working with cyber security and privacy issues to discuss and enhance their bilateral cooperation. Similarly, the Open Cyber Camp EU-U.S. invites entrepreneurs, industry leaders, and researchers to gather and identify new challenges to cyber security, enhance privacy-protection cooperation, and build partnerships across the Atlantic.[122]

As in its partnership with the United States, the EU is also developing research projects with Japan. The Nippon-European Cyberdefence-Oriented Multilayer Threat Analysis (NECOMA) project, which ran between 2013 and 2016, is an example. The project, which focused on data collection and threat analysis, was co-funded by the EU's Seventh Framework Programme and the Strategic International Collaborative R&D Promotion Project of the Japanese Ministry of Internal Affairs and Communication.[123] Another example is the Horizon 2020-funded EUNITY Cybersecurity and Privacy Dialogue between Europe and Japan which "aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions".[124] Overall, there are around 75 joint EU-Japan projects operating under the auspices of Horizon 2020 nowadays. ICT is the most popular area of research.[125] The EU is well-aware of the importance of cyber security research and cooperation with its strategic partners. That was illustrated in the Call for EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation issued under H2020 in 2016. Two of its three strands of proposals were for projects of international dialogue with Japan and the USA[126].

The importance of research cooperation between the EU and Japan has also been affirmed in ICT Strategies Workshops. During these workshops, government-to-government and industry-to-government meetings and expert-level gatherings are organised on topics such as the digital economy, artificial intelligence and cyber security. For instance, during the Seventh ICT Strategies Workshop in April 2018, the EU and Japan proposed that they should "explore participation in research" as a follow-up activity.[127]

Last but not least, the Cyber Diplomacy and Resilience Clusters (EU Cyber Direct) should be mentioned. Since 2018, Cyber Direct's purpose has been to establish a "one-stop-shop" for official cyber dialogues with the EU's strategic partners (Brazil, China, India, Japan, South Korea, and the United States) as well as Latin America and the Asia-Pacific region more broadly. Recognizing that "the EU's role, its policies and institutional set up are still

[121] AEGIS: About us. Retrieved from: http://aegis-project.org/about-us/

[122] AEGIS: Home. Retrieved from: http://aegis-project.org/

[123] NECOMA: Home. Retrieved from: http://www.necoma-project.eu/

[124] EUNITY: Home. Retrieved from: https://www.eunity-project.eu/en/

[125] Japan - National Contact Point: Summary of EU-Japan collaborations through Horizon 2020 and FP7. Retrieved from: https://www.ncp-japan.jp/horizon-2020/summary-eu-japan-collaborations-horizon-2020-fp7

[126] European Commission (14 October 2015): EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/ds-05-2016

[127] Delegation of the EU to Japan, press release (2018): EU and Japan intensify bilateral cooperation on digital economy issues. Retrieved from: https://eeas.europa.eu/delegations/japan/43252/eu-and-japan-intensify-bilateral-cooperation-digital-economy-issues_en

poorly understood in other parts of the world",[128] the project gathers together members of the EU Institute for Security Studies (EU ISS), the German Marshall Fund of the United States (GMF) and the Stiftung Neue Verantwortung (SNV). In addition to publishing research and analysis papers, EU Cyber Direct organises regular workshops, conferences and meetings. Its last EU Cyber Forum invited actors from several different sectors: diplomats from Brazil, Ireland and Finland, academics and experts, representatives of the EU administrations, etc. "This whole-of-the-EU approach ensures that the [scientific] agenda of the Forum remains policy relevant and feeds directly into the policy dialogues and cooperative arrangements that the EU pursues with partner countries".[129] The Cyber Forum is a major initiative for EU cyber science diplomacy.

[128] EU Cyber Direct (9 April 2019): EU Cyber Forum 2019. Retrieved from: https://eucyberdirect.eu/content_events/eu-cyber-forum-2019/
[129] Ibid.

6. Meta-perspective

The case studies above (especially the national ones) have certain common aspects, besides being driven by foreign policy as an increasingly salient security issue, which deserve consideration. The first is the role of diplomats who have a particular focus on cyber security (most often with title "cyber attachés"). In the Czech case, these are cyber experts delegated from NCISA and deployed in three countries that are key to the Czech Republic's international cyber security. Germany has a much wider network of cyber attachés. The Federal Foreign Office currently deploys twenty cyber diplomats around the world. In contrast, France has decided to use a slightly different model. Besides two full-time employees who are focused on cyber security issues at the MEAE and a cyber counsellor deployed with the French Permanent Representation in Brussels, France has also named a digital ambassador, who is attached to the MEAE. Each of the countries studied has diplomats with a particular responsibility for cyber security issues. However, they are not necessarily cyber experts themselves.

Besides the cyber diplomats, all three states have also deployed science diplomats. France has rich experience in this regard. Similarly, Germany has a broad network of science attachés posted at thirty embassies abroad. These diplomats are not all career diplomats. A number of them are civil servants dispatched from the Federal Ministry of Education and Research. The Czech Republic is the least advanced in this regard, having only two science diplomats and no plans to deploy more.

Given that the cyber attachés and science diplomats are often deployed in the same embassies, a relevant question is how these two positions interact. Do they overlap and do they coexist in harmony? For example, the Czech Republic's two diplomats are deployed in same embassy. They work more or less symbiotically if the situation requires it. Their relationships are not governed by a clear, institutionalised division of their agendas and responsibilities but are based on mutual personal agreement. In comparison, the responsibilities of German science diplomats and cyber attachés are very clearly defined. However, there are no predefined cooperation schemes or interfaces between them. Their cooperation depends on the interest of the involved personnel in linking their spheres of responsibility.

The countries also share certain limitations on science diplomacy in the area of cyber security. For example, all the case studies indicate that the three countries and the EU have no clear idea what science diplomacy in relation to cyber security encompasses and no strategic approach to linking the two disciplines. Moreover, the Czech and German cases reveal that those two countries do not have a clear government-wide understanding of what exactly is meant by the term "science diplomacy" and what activities it should involve.

Furthermore, all of the national cases show that the relationship between diplomats and scientists remains quite narrow and involves very few actors. Their relationships are often informal and very weakly institutionalised. This inevitably leads to the conclusion that in most cases, cooperation very much depends on the personal interests and previous experience of those in charge, who are able to determine their own approach to diplomacy and undertake particular activities independently. This often results in cooperation between government structures and academia that is more on a case-by-case basis than in a sustainable manner.

The Czech Republic, France and Germany are clearly countries with very different levels of advancement when it comes to promotion of science diplomacy in relation to cyber security. As seen in the sections above, the understanding of science diplomacy in this area includes elements of science in diplomacy, science for diplomacy, and global challenges. France is the most focused on this type of diplomacy of the three countries. Germany has apparently realized its importance and is planning to expand it (e.g., by establishing a new German Institute for International Cyber Security). The least advanced of the three countries is the Czech Republic, which despite its cyber security potential, does

not possess a sustainable framework for science diplomacy. However, no matter how far advanced the three countries may be, their science diplomacy shares certain common aspects in its relation to cyber security. These include the roles played by their cyber and science diplomats and the limits of their science diplomacy in the cyber realm.

Trying to synthesize a conclusion from the different dimensions displayed by the case of the EU, the following three elements should be highlighted. First, ongoing EU activities are aimed at more strategic and better coordinated responses to the challenges of science and technology. Motivated by its stated strategy of achieving technological autonomy, the EU funds policies that have several objectives: better integration of Member States' national resources; facilitation of trans-sectorial synergies between actors from industries, laboratories and institutions; and, inside some of the funded projects, better cooperation between disciplines (e.g., computer and social sciences).

Second, the EU's scientific diplomacy agenda is being institutionalized. Even if it is far too early to fully assess this dynamic, several recent initiatives seem to be trying to bring various types of scientific expertise into diplomatic initiatives. One indication of the development of the EU's science diplomacy is that researchers involved into some of the projects use diplomatic vocabulary to describe their own work, for example, the term "track 1.5" used by a French interviewee.[130]

Third, we can identify two main challenges for cyber science diplomacy. For one, there is a question about how the goal of "strategic autonomy" might hinder international cooperation with third countries. Strategic autonomy may motivate synergies at EU level, but the way it can be reconciled with bilateral initiatives with other countries still needs to be assessed. Another question is whether the science diplomacy practiced in some specific institutions (such as EU ISS) and some projects (like the EU's Cyber Direct) will now be mobilised in other EU official arenas. For example, TCPRI has been described as an interesting "pilot experience" but those experiences have never been translated into general practice.[131] Relationships between participants in the scientific projects and the EU institutions vary significantly. As one interviewee said, "the EEAS has its own agenda".[132] Another difficulty is turnover among EU officials' working in various departments of the Commission and the EEAS, which means regularly rebuilding relationships and mutual understanding of technical issues.[133] For those reasons, science diplomacy in the cyber field on the EU level remains weakly institutionalised.

[130] Interview, EU Cyber Direct, 2 May 2019.
[131] Interview, TCPRI, 12 April 2019.
[132] Ibid.
[133] Interview, EEAS, 24 April 2019.

7. References

AEGIS: Home. Retrieved from: http://aegis-project.org/

Amires: Cybersecurity Projects within H2020. Retrieved from: http://amires.eu/cyber-security-projects-within-h2020/

ANSSI (2011): Défense et sécurité des systèmes d'information - Stratégie de la France.

ANSSI (2015): Stratégie Nationale pour la sécurité du numérique.

ANSSI (2017): Conférence "Construire la paix et la sécurité internationals de la société numérique". Retrieved from: https://www.ssi.gouv.fr/actualite/conference-construire-la-paix-et-la-securite-internationales-de-la-societe-numerique-le-programme-maintenant-disponible/

ANSSI: A Word from the Director General. Retrieved from: https://www.ssi.gouv.fr/en/mission/word-from-director-general/

Appel de Paris (2018).

BIC: Home. Retrieved from: http://www.bic-trust.eu/index.html

BITKOM: About. Retrieved from: https://www.bitkom.org/EN/About-us/About-us.html as accessed 2 May 2019.

Chaire Castex de Cyberstrategie: The Aims of the Castex Chair. Retrieved from: http://www.cyberstrategie.org/?q=en/the-aims-of-the-castex-chair

Council of the EU (20 November 2010): EU-US Summit, joint statement. Retrieved from: http://europa.eu/rapid/press-release_PRES-10-315_en.htm?locale=en

Council of the EU, press release (2019): EU to pool and network its cybersecurity expertise – Council agrees its position on cybersecurity centres. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/

Cyber and Information Domain Service Headquarters, Press and Information Centre: Cyber and Information Domain. Retrieved from: http://cir.bundeswehr.de/resource/resource/YjR0QzY3aWZvTE4yUHd5Vk55eFhUZFo5dGh3aGZlRTE1VnNvSDFHRnNjUFVxa1l1S3hITWlWRFlRM3ZUSUVjM0NxYXNjck1BVG1RdFBZdWlqNTZ2d3lVY2N0TzRuOE9zakR5STNzcklUTWs9/Flyer_CIR_engl.pdf as accessed 2 May 2019.

Cyber Security Agency of Singapore: Singapore Signs Joint Declaration of Intent on Cybersecurity Cooperation with Germany. Retrieved from: https://www.csa.gov.sg/news/press-releases/singapore-signs-joint-declaration-of-intent-on-cybersecurity-cooperation-with-germany as accessed 2 May 2019.

CzechInvest: Research and Development in the Czech Republic. Retrieved from: http://www.czech-research.com/ as accessed 14 April 2019.

Delegation of the EU to Japan, press release (2018): EU and Japan intensify bilateral cooperation on digital economy issues. Retrieved from: https://eeas.europa.eu/delegations/japan/43252/eu-and-japan-intensify-bilateral-cooperation-digital-economy-issues_en

Deutsche Telekom, T-Labs: Über uns https://laboratories.telekom.com/ as accessed 2 May 2019.

Deutsche Telekom: Geschäftsbericht 2017. Mitarbeiterstatistik. Retrieved from: https://www.geschaeftsbericht.telekom.com/site0218/lagebericht/mitarbeiter/mitarbeiterstatistik.html as accessed 2 May 2019.

ECHO (25 February 2019): ECHO Project Press Release. Retrieved from: https://www.echonetwork.eu/wp-content/uploads/2019/02/Echo_press_relase_2502.pdf

EEAS, press release (14 March 2018): 3rd EU-Japan Cyber Dialogue – Joint Elements. Retrieved from: https://eeas.europa.eu/topics/eu-international-cyberspace-policy/41330/3rd-eu-%E2%80%93-japan-cyber-dialogue-joint-elements_en

EEAS, press release (16 December 2016): EU-US Cyber Dialogue. Retrieved from: https://eeas.europa.eu/headquarters/headquarters-homepage_en/18132/EU-U.S.%20Cyber%20Dialogue

Embassy of France in Tokyo: Présentation des services. Retrieved from: https://jp.ambafrance.org/Presentation-des-services#Service-pour-la-science-et-la-technologie

EU Cyber Direct (9 April 2019): EU Cyber Forum 2019. Retrieved from: https://eucyberdirect.eu/content_events/eu-cyber-forum-2019/

EUNITY: Home. Retrieved from: https://www.eunity-project.eu/en/

European Commission – Cordis: BIC – Objective. Retrieved from: https://cordis.europa.eu/project/rcn/95486/factsheet/en

European Commission – Cordis: FIRE – Objective. Retrieved from: https://cordis.europa.eu/project/rcn/105736/factsheet/en

European Commission (14 October 2015): EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/ds-05-2016

European Commission (2013): Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

European Commission press release (5 July 2016): Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats. Retrieved from: http://europa.eu/rapid/press-release_IP-16-2321_en.htm

European Commission: Cybersecurity. Updated 16 April 2018. Retrieved from: https://ec.europa.eu/digital-single-market/en/cyber-security

European Commission: Cybersecurity: Horizon 2020 Pilot Projects. Retrieved from: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57561

European Commission: Proposal for a European Cybersecurity Competence Network and Centre. Updated September 2018. Retrieved from: https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

European Council and Council of the EU (19 June 2017): Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanction. Retrieved from: https://www.consilium.europa.eu/fr/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

European Council, Preparatory Bodies: Horizontal Working Party on Cyber Issues (HWP). Retrieved from: https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-cyber-issues/ as accessed 2 May 2019.

Federal Foreign Office, Außen- und Europapolitik: Internationale Wissenschaftlich-Technologische Zusammenarbeit. Retrieved from: https://www.auswaertiges-amt.de/de/aussenpolitik/themen/aussenwirtschaft/forschungtechnologie/wissenschaftlichtechnologischezusammenarbeit-node as accessed 23 May 2019.

Federal Foreign Office, Foreign and European Policy (2017): International Cyber Policy. Retrieved from: https://www.auswaertiges-amt.de/en/aussenpolitik/themen/cyber-aussenpolitik as accessed 23 May 2019.

Federal Ministry for Economic Affairs and Energy (2018): Strategie Künstliche Intelligenz der Bundesregierung.

Federal Ministry of Defence (2016): The White Paper on Security Policy and the Future of the Bundeswehr.

Federal Ministry of Education and Research (2018): Cybersecurity Research – Proposal to develop the synergy between France and Germany. Position paper by the expert group. Retrieved from: www.bmbf.de.

Federal Ministry of Education and Research (2018): Research for Civil Security 2018–2023 – A Federal Government Framework Programme.

Federal Ministry of the Interior (2016): National Cyber Security Strategy for Germany.

German National Office for Information Security, BSI: Act to Strengthen the Security of Federal Information Technology. Retrieved from: https://www.bsi.bund.de/EN/TheBSI/BSIAct/bsiact_node.html as accessed 2 May 2019.

Government of the Czech Republic (2016): National Research, Development and Innovation Policy of the Czech Republic 2016–2020. Retrieved from: https://www.vyzkum.cz/FrontClanek.aspx?idsekce=782691

Government of the Czech Republic: Deputy Prime Minister Bělobrádek Officially Introduced the Second Science Diplomat. Retrieved from: https://www.vyzkum.cz/FrontAktualita.aspx?aktualita=807455 as accessed 12 April 2019.

INRIA (January 2019): Cybersecurity. Current challenges and Inria's research directions, White Book No. 3.

INRIA: Joint Collaboration between France and Japan on Cybersecurity Research. Updated March 2019. Retrieved from : https://project.inria.fr/FranceJapanICST/fr/

Japan - National Contact Point: Summary of EU-Japan collaborations through Horizon 2020 and FP7. Retrieved from: https://www.ncp-japan.jp/horizon-2020/summary-eu-japan-collaborations-horizon-2020-fp7

Kadlecová, Lucie, Daniel Bagge, Michaela Semecká, Václav Borovička (2017): The Czech Republic: A Case of a Comprehensive Approach toward Cyberspace. Tallinn: NATO CCDCOE. Retrieved from: https://ccdcoe.org/library/publications/the-czech-republic-a-case-of-a-comprehensive-approach-toward-cyberspace/

Majer, Vladimír (2017): Science Diplomacy according to Czech Republic. In: Česká pozice. Retrieved from: http://ceskapozice.lidovky.cz/vedecka-diplomacie-po-cesku-dfz-/tema.aspx?c=A170720_232214_pozice-tema_lube

MEAE - Direction générale de la mondialisation, du développement et des partenariats (2013): Une diplomatie scientifique pour la France. January 2013. Retrieved from: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/

MEAE (2017): Stratégie internationale de la France pour le numérique.

MEAE: La France et la cybersécurité. Updated May 2019. Retrieved from: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-et-securite/cybersecurite/

MEAE: Scientific Diplomacy. Retrieved from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/scientific-diplomacy/

Ministère des Armées (2017): Revue stratégique de défense et de sécurité nationale.

Ministry of Foreign Affairs of the Czech Republic: Projects of Economic Diplomacy for 2019. Retrieved from: https://www.mzv.cz/ekonomika/cz/servis_exporterum/projekty_ekonomicke_diplomacie/projekty_ekonomicke_diplomacie_pro_rok.html

Ministry of the Interior of the Czech Republic (2017): Interdepartmental Concept of Support for Security Research of the Czech Republic. Retrieved from: https://www.mvcr.cz/vyzkum/clanek/koncepce-meziresortni-koncepce-podpory-bezpecnostniho-vyzkumu-cr.aspx

MN CD ET: Project. Retrieved from: https://mncdet.wixsite.com/mncdet-nato as accessed 12 April 2019.

National Security Authority, National Cyber Security Centre (2015): National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf

NCISA: Research. Retrieved from: https://nukib.cz/cs/informacni-servis/vyzkum-nukib/ as accessed 14 April 2019.

NECOMA: Home. Retrieved from: http://www.necoma-project.eu/

Renard, Thomas (2018): EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. In: European Politics and Society. 19(3), pp. 321-337.

SGDSN (2008): Livre Blanc sur la Défense et la Sécurité Nationale.

SGDSN (2013): Livre Blanc sur la Défense et la Sécurité Nationale.

SGDSN (2018): Revue stratégique de Cyberdéfense.

SNV (2018): EU-US Cyber Diplomacy Workshop on Transatlantic Cyber Policy Research Initiative. Retrieved from: https://www.stiftung-nv.de/en/node/2484

Technology Agency of the Czech Republic (2018): Programme Delta 2. Retrieved from: https://www.tacr.cz/index.php/en/26-programy/delta/1469-delta-delta-2-guidepost.html

The IT Law Wiki, wikia: National Cyber Security Council. Retrieved from: https://itlaw.wikia.org/wiki/National_Cyber_Security_Council as accessed 2 May 2019.

Interviews Czech Republic

Interview, CzechInvest, Prague, 29 November 2018.

Interview, Ministry of Foreign Affairs of the Czech Republic, Prague, 5 December 2018.

Interview, Masaryk University, Brno, 19 March 2019.

Interview No. 1, NCISA, Brno, 17 January 2019.

Interview No. 2, NCISA, Brno, 17 January 2019.

Interview No. 3, NCISA, Prague, 26 March 2019.

Interview No. 4, NCISA, Prague, 26 March 2019.

Interviews Germany

Interview 1, a representative of German public sector, Bonn, 9 February 2019.

Interview 2, a representative of German public sector, Bonn, 22 February 2019.

Interview 3, a representative of German public sector, Bonn/Berlin, 5 April 2019.

Interview 4, a representative of German public sector, Bonn/Berlin, 2 April 2019.

Interview 5, a representative of the German private sector, Bonn, 1 February 2019.

Interviews France

Interview, INRIA, 6 February 2019.

Interview, MEAE, 9 April 2019.

Interview, Castex Chair, 5 February 2019.

Interview, Castex Chair, 23 April 2019.

Interview, French Permanent Representation, 24 April 2019.

Interviews European Union

Interview, SPARTA, researcher, 6 February 2019.

Interview, TCPRI, 12 April 2019.

Interview, Egmont Institute, cyber expert, 23 April 2019.

Interview, EEAS, cyber expert, 24 April 2019.

Interview, EU Cyber Direct, researcher, 2 May 2019.

Other Interviews

TrendMicro private expert (central player of the French cyber field)

Le Monde specialist for cyber issues

CEIS expert (a think tank responsible for relations with MinDef)

ANSSI (directorate for international affairs)

ANSSI (expertise directorate)

CESDIP (researcher, political science, he previously held the "Cybersecurity and Cyberdefense" Chair of Saint-Cyr-Coëtquidan military schools)

CRESC (researcher, also teacher in Saint-Cyr-Coëtquidan military schools)

Chaire CASTEX (researcher, geostrategy)

Chaire CASTEX/Paris 8 (researcher, geostrategy)

AMNESCYS & CESICE (researcher, international law)

AMNESCYS (researcher, computer sciences, also member of the Castex Chair)

Observations

Symposium "Research methods into cybersecurity in the humanities and social sciences", CESDIP/University of Saint-Quentin, 19 November 2018.

Meeting Cybersécurité – Cybercercle/Nano-Innov', Paris Saclay, 22 November 2018.

International Cybersecurity Forum, Lille, 17-18 January 2019.