Dóra Molnár

European Cyber Diplomacy Landscape – France, the United Kingdom and Germany

Introduction

When it comes to cybersecurity, the saying “as many states, so many approaches” is certainly true. This is true not only globally, but also for European states. States have recognised the growing importance of this area at different times and have described a different trajectory in both the development of their cybersecurity strategic culture and its implementation. Accordingly, the importance of cyber diplomacy varies from state to state, although it is an undoubted fact that most states now emphasise the strategic importance of cyber relations, the need for cooperation and the need to establish rules of conduct in cyberspace at the strategic level. However, the proposed solutions are very different. For example, one group of states considers it necessary to create a comprehensive cyber convention, while others strongly oppose it along arguments based on the characteristics of cyber weapons.[1] Most states in the Western world are pushing for a multi-stakeholder governance model of the Internet, while the developing world, led by China and supported by Russia, is in favour of a multilateral solution in every possible forum. However, in addition to the many different approaches, there are several commonalities in public policies. Most states seek to make the most of the opportunities offered by international fora and organisations, but they also seek to build the widest possible network of bilateral contacts. The fault lines between individual states are well delineated on the basis of whether they manage to bring a bilateral cyber agreement under the roof.

The study examines three European states. Today, the United Kingdom is the world’s leading cyber state, so it is impossible to ignore the British cyber diplomatic solutions. However, when it comes to diplomacy, France comes to

[1] These include, for example, the unresolved nature of control issues and the difficulty of rapid technological change and adaptation. See Fahad Nabeel: International Cyber Regime: A Comparative Analysis of the US–China–Russia Approaches. *Stratagem,* 1, no. 2 (2018). 8–27.

https://doi.org/10.36250/01039_03

mind as the first European state, so I will also start my study by presenting French characteristics. The third state surveyed is Germany, due to the country's leading European position and the unique intertwining of the economy and cyber politics. Each of the states surveyed has been advocating the need to regulate cyberspace for years, most recently joining the Joint Declaration on Advancing Responsible State Behaviour in Cyberspace on 23 September 2019, along with a further 24 states.[2] The U.S.-initiated statement underlined the need for a concerted and coordinated cyber effort to protect citizens, among other things, from a series of cyberattacks – adding that the attacks are being carried out by Russia and other adversaries. It has also been declared that inappropriate cyberspace behaviour will have consequences. In the following, I present the international activities of the three states and/or the main actors of the network of bilateral contacts, based on the national cyber strategies.

France as a Cyber Diplomatic Power

Perhaps it is no exaggeration to say that France has been a stronghold of diplomacy for centuries, and that the French are great masters of the use of "soft" tools in politics. The country's strength is given by its global role, based on its extensive diplomatic network: it has an unparalleled membership in multilateral and international organisations, with the highest number of foreign cultural missions and the 5th largest donor state.[3] It is therefore not surprising that French politics prefers to use the tools of diplomacy in cyberspace effectively – so much so that it is at the forefront of this field at European level. This justifies me starting my study of European countries with France, even if there is another European state in terms of cyber power potential that is ahead of the country.

The need for international cooperation in cyberspace as one of the necessary areas for action is already reflected in the first cyber strategy, *Protection and Security of Information Systems: A Strategy for France,* published in 2011.[4] This is specified in Senate Information Report No. 681, adopted in 2012, by

[2] U.S. Department of State: *Joint Statement on Advancing Responsible State Behavior in Cyberspace.* 23 September 2019.

[3] Consulat Général de France á Ekaterinbourg: *La diplomatie française à l'ère numérique.* 29 May 2019.

[4] Agence nationale de la sécurité des systèmes d'information: *Défense et sécurité des systèmes d'information. Stratégie de la France.* 2011.

emphasising the importance of bilateral relations as one of the ten priorities, and calling for joint action with the Organization for North Atlantic Cooperation (NATO) and the European Union (EU), dialogue with China and Russia, and supports the adoption of international confidence-building measures.[5] The 2013 White Paper emphasises the need for a "global governmental approach" to combat cyberattacks, in which France builds on its diplomatic, legal and political instruments.[6]

The country's cyber strategy was released in 2015 under the title *National Digital Security Strategy.*[7] The strategy sets out five main objectives, the fifth of which is entitled *Europe, Digital Strategic Autonomy, Cyberspace Stability.* France intends to participate in Europe's digital transformation through its allied relations, in three main ways: by setting out a roadmap for a European strategy with other EU volunteers, by strengthening the French presence and influence in international cyber talks, and by supporting other states in building cyber capabilities, thereby contributing to the global stability of cyberspace. According to the strategy, the main venues for increasing influence among the international organisations are the United Nations (hereinafter: the UN) and the Organization for Security and Cooperation in Europe (hereinafter: the OSCE), active participation in bilateral relations in the framework of diplomatic dialogue at ministerial level and in informal international fora with political decision-makers and academia. The area of cyber diplomacy was centralised to implement the strategy, and in 2015 the position of ambassador for cyber diplomacy and the digital economy was set up in the Ministry of Foreign Affairs.[8]

Since the adoption of the 2015 strategy, the international environment has changed significantly. It is enough to think of the series of cyberattacks following the terrorist attack on Charlie Hebdo or against the television channel TV5. The events also shed new light on the issue of cybersecurity in France and encouraged the country to take more active and vigorous national and international action.

The new approach is reflected in the Offensive Cyber Operations Doctrine, published on 18 January 2018, about three weeks before the release of the Cyber

[5] Sénat: *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense.* Par le Sénateur M. Jean-Marie Bockel. Sénat session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012.

[6] Ministère des Armées: *Livre Blanc. Défense et sécurité nationale 2013.* Paris.

[7] SGDSN: *La stratégie nationale pour la sécurité du numérique.* 2015.

[8] The position, which has been called Digital Ambassador since 22 November 2017, was filled by David Martinon.

Defence Strategic Review. In the document, France openly states that cyber capabilities are part of its military activities and are ready to be deployed if necessary. This certainly marks a turning point in French cyber politics, which has so far been characterised by discreet diplomatic actions: even in case of blatant cyber conflicts such as the Russian-sponsored cyberattack on the Navy to find out about oil supply channels, France did not use offensive rhetoric, but sought to defuse tensions by using the means of dialogue.[9]

On 8 February 2018, the latest Cyber Defence Document entitled *Cyber Defence Strategic Review* was issued as the official material summarising the country's cyber defence ambitions.[10] Also known as the *White Paper on Cyber Defence,* the document sets out in several chapters the need for some cyber diplomatic action and sets out France's position on the issue. There is a separate chapter on international negotiations on the regulation of cyberspace, highlighting the role of the UN and the Group of Governmental Experts (GGE) and their achievements since 2013. At the 2016–2017 session, France put forward a separate proposal for a deeper regulation of the non-refoulement ban, which, although supported by the participating states, was stalled due to differing views on how to apply international law. Another chapter shows how the country performs internationally in cyberspace. It promotes dialogue and cooperation with its allies in order to prevent cyber conflicts, urges the regulation of cyberspace and aims to ensure European security and autonomy in cyberspace as well. From among its bilateral relationships it highlights its cyber relations with the United States,[11] China, India,[12] Brazil and Japan, adding that it will continue to cultivate deep ties with its Western allies, but will place increasing emphasis on the sub-Saharan region, where it urges the establishment of relations with the Francophone states. European cyber relations need to be organised along three issues: technical, regulatory and capacity issues, which require the formulation

[9] Arthur P. B. Laudrain: France's New Offensive Cyber Doctrine. *Lawfare,* 26 February 2019.

[10] SGDSN: *Revue stratégique de cyberdéfense.* 12 February 2018.

[11] The third stop of the Franco–American cyber dialogue was held on 22 January 2020 in Paris. The central topic of the meeting was the applicability of international law to cyberspace. Ministère de l'Europe et des Affaires Étrangères: *Troisième dialogue stratégique France–*États-*Unis en matière de cybersécurité (Paris, 22 janvier 2020).*

[12] The India–France Bilateral Cyber Dialogue was held for the third time on 20 June 2019, discussing primarily issues related to cyber norms. The importance of bilateral cyber relations is well signalled by India's invitation to the 2019 G7 summit from France, which held the presidency in 2019. Ministère de l'Europe et des Affaires Étrangères: *Indo–French Bilateral Cyber Dialogue (Paris, 20 June 2019).*

and adoption of common ground. The Franco–German system of relations occupies a prominent place in both bilateral and European relations. Cooperation between the two countries is very intensive and extensive, as evidenced by the two joint reports published so far.[13] Finally, the document calls for the adoption of an action doctrine that sets out fundamental issues such as the classification system for cyberattacks and the range of responses to cyber incidents. A global system for regulating cyberspace can only be implemented along the lines of principles such as prevention, cooperation and stability.

Despite a more "offensive" attitude, diplomatic moves will certainly continue to play a key role in French politics in the future. It is no coincidence that France is one of the most active Member States in various international organisations when it comes to cybersecurity issues. Not only in the UN, as discussed above in relation to the GGE, but also in NATO, the G7 and the OSCE.[14] In the latter organisation, France played a very important role in the adoption of the two packages of confidence-building measures related to cybersecurity. With regard to the French participation in the G7, I would like to highlight the meeting held in the small French town of Dinard on 5–6 April 2019, where the so-called Dinard Declaration on the Initiation of Cyberspace Rules was accepted.[15] It welcomed the UN General Assembly's supportive approach to the applicability of international law in cyberspace and reaffirmed their intention to promote an open, secure, stable, accessible and peaceful cyberspace. At the same time, they reaffirmed their intention to formulate a Cyber Norm Initiative – CNI, which was finalised on 26 August 2019 with ten basic rules applicable in cyberspace.[16] All of this fits well with the success story of French soft politics, although it should be added that there was no precedent for the adoption of such an initiative. From 12 to 14 November 2018, the UNESCO Headquarters in Paris hosted the thirteenth annual meeting of the Internet Governance Forum, where French President Emmanuel Macron himself announced the Paris Call for Confidence

[13] Agence nationale de la sécurité des systèmes d'information: *ANSSI/BSI Common Situational Picture.* Vol. 1 – July 2018; Agence nationale de la sécurité des systèmes d'information: *Second Edition of the Franco–German Common Situational Picture.* 21 May 2019.

[14] Ministère de l'Europe et des Affaires Étrangères: *La France et la cybersécurité.* s. a.

[15] Ministère de l'Europe et des Affaires *Étrangères*: *Dinard Declaration on the Cyber Norm Initiative.* 06 April 2019.

[16] Ministère de l'Europe et des Affaires *Étrangères*: *Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques.* 26 August 2019.

and Security in Cyberspace.[17] The widespread acceptance of the call is well indicated by the fact that it was immediately supported by more than 500 entities (state, organisation and company).[18] However, the completeness of the picture also includes the fact that each of the three "big" states rejected the initiative, torpedoing its global acceptability. With the call and a number of similar initiatives, France aims to see the country as a cyber power worldwide. Perhaps this goal also guided the country on 9 September 2019, when the French Ministry of Defence set out in an official document its views on how international law, according to France, could be applied in cyberspace[19] – thereby also taking on a pioneering role in cyber diplomacy.

Germany

Although Germany has been actively involved in UN cybersecurity consultations and other bilateral and multilateral fora since 2004, cooperation has been limited to technical issues. Although the first German cybersecurity strategy in 2011 mentioned the international and diplomatic dimensions of cybersecurity, until the Snowden case, Germany did not play a significant role in cyberspace. Only after the case Germany together with Brazil, due to the involvement of German Chancellor Angela Merkel, initiated the adoption of a UN resolution on the protection and inviolability of the right to privacy in the digital age, which resulted in the adoption of UN General Assembly Resolution No. 68/167 on 18 December 2013. This was a major cyber diplomatic success for Germany, especially because it managed to raise this issue to global level with South American support. From then on, Germany has become an active supporter of cyber diplomacy. In 2016, under the German chairmanship of the OSCE, the second package of confidence-building measures in cyberspace was adopted, and in 2016–2017, German diplomatic representatives also chaired the UN GGE.

[17] Ministère de l'Europe et des Affaires Étrangères: *Appel de Paris pour la confiance et la sécurité dans le cyberespace.* 12 November 2018.

[18] Ministère de l'Europe et des Affaires Étrangères: *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace. Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018).*

[19] Przemyslaw Rogusky: France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I. *Opinio Juris,* 24 September 2019.

The foundations for increasingly active German action must be found in the country's cybersecurity strategy. In 2016, the country's second cyber strategy was released[20] which already highlights the importance of cooperation, which, however, must not be limited to national frameworks, but must establish pan-European and even global channels of cooperation. The document identifies four areas for action, one of which is the appropriate positioning of Germany in European and international cybersecurity policy discussions. This clearly shows that cyber diplomacy has established itself as a priority area and has become a fundamental factor influencing the security of a country. As part of this, Germany also emphasises the importance of bilateral partnerships, especially in areas such as information sharing and the coordination of security issues related to cross-border services, capacity sharing and in the field of development cooperation, where security and confidence-building measures are the key to success.

Germany is also gradually putting the strategy into practice with bilateral relations playing an enhanced role. The *United States* is a key strategic partner, so it is no coincidence that their cyber dialogue also has a long and meaningful history. Since 2012, a bilateral cyber meeting has been held annually, one year in Washington, the other in Berlin. During the meetings, issues such as the applicability of international law in cyberspace or the online enforcement of human rights are discussed like in 2016, but their common thinking of the multi-stakeholder model of cyberspace is also well established.[21] A consensus was reached with *China* in November 2016 that the two states would continue the dialogue on cyber issues through a special mechanism, but no bilateral agreement has been signed to date.[22] Most recently, Chancellor Merkel held talks in China in January 2020 to create a German–Chinese cyber agreement (similar to the U.S.–China agreement), but its precondition is the introduction of a "no spy" clause due to the American Huawei scandal. However, when asked about the convention, the Chancellor only said diplomatically that Germany and China have been constantly discussing a number of bilateral and international issues with each

[20] Federal Ministry of the Interior: *Cyber-Sicherheitsstrategie für Deutschland 2016* [Cybersecurity Strategy for Germany 2016].

[21] U.S. Department of State: *Joint Statement on U.S.–Germany Cyber Bilateral Meeting.* 24 March 2016.

[22] Christopher Burgess: Dissecting China's Global Bilateral Cybersecurity Strategy. *Security Boulevard,* 09 October 2016.

other on several levels.[23] At the same time, the German bilateral palette is not limited to the large partner states, but presents an extremely colourful picture. Germany, for example, has good bilateral cyber relations with Singapore. In 2017, the Prime Minister of Singapore paid a visit to Germany, during which the two sides signed a joint memorandum of understanding on cybersecurity cooperation in areas such as information sharing or joint research. The visit was reciprocated by Chancellor Merkel in June 2018, and the leaders of the two countries also concluded a defence treaty with a separate cyber clause.[24]

Germany is active in discussing cybersecurity issues in a number of international institutions, but perhaps the role of the *OSCE* stands out among all these actions. At the same time, Germany was predestined to take the lead in OSCE initiatives. On the one hand, because historically they are linked by political and economic threads to both the East and the West, and the OSCE also connects the leading powers in these regions. On the other hand, because Germany is a leading state in this area – it is enough to think about the technical standards and regulations set up in the field of data protection. Thirdly, because Germany participates effectively in organisations (such as the GGE) that set standards and rules in cyberspace, furthermore it can also benefit from the experience it has gained here.[25]

In 2013, the OSCE developed the first package of confidence-building measures in cyberspace, which provided an appropriate basis for moving forward. During the 2016 German OSCE Chairmanship, the possible scope of confidence- and security-building measures was discussed separately in all three baskets. For the first basket, only a series of voluntary agreements on military cooperation between Member States were recorded in 2013. It was agreed that the OSCE would be used as a platform to exchange information on cyberattacks and to mutually support the expansion of national capabilities. The German presidency explicitly aimed to involve engineers (primarily IT professionals) in cyber diplomacy (not just concerning the first basket), which is expected to have the effect of reducing diplomatic tensions, such as the developments at the Pugwash conferences since the 1950s. The German Information Security Act,

[23] Guy Chazan: German Cyber Security Chief Backs 5G ‘No Spy’ Deal over Huawei. *Financial Times,* 28 February 2020.

[24] Prashanth Parameswaran: Singapore–Germany Cyber Cooperation in Focus with Introductory Visit. *The Diplomat,* 14 August 2018.

[25] German Institute for International and Security Affairs: *Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016.* Berlin, 11 November 2015.

adopted in 2015, which set higher security requirements for critical infrastructure protection, served as a reference point for the second steps in the economic basket. German law also served as a reference when the NIS Directive was drafted. The central German cyber body, the Federal Office for Information Security (BSI)[26] has served as a model of technical expertise for many OSCE partners.

All these developments open a new horizon in the context of OSCE economic cooperation. In the case of the third basket, the issue of human rights, including freedom of expression on the Internet, is problematic. Above all, the German Presidency had to find an answer to the dilemma of censorship, network surveillance and copyright issues.

Germany makes the regulation of cyberspace a top foreign policy priority. He strongly advocates that global issues can only be resolved through common regulation – and this includes cybersecurity. The problem cannot be tackled at national level alone, but requires close cooperation between states, international organisations, NGOs and academia. It declares the applicability of international law in cyberspace and supports the multilateral approach.[27] In any case, it should be considered a diplomatic success that in November 2019, Germany was able to give home to the UN Internet Governance Forum.

The Leading (European) Cyber Power: The United Kingdom

The U.K., like the great powers, recognised the importance of cybersecurity and cyber diplomacy at an early stage, which it reflected in its strategic documents and successfully put into practice. The first cybersecurity strategy was issued in 2009, but was soon replaced in 2011 by a new strategy outlining the main guidelines, objectives and conditions for implementation over a five-year period. The title of the strategy is *Protecting and Promoting the UK in a Digital World.* The document[28] sets out four objectives, the second of which has a role to play in cyber diplomacy. The stated goal of the country is to be able to respond flexibly to cyber threats and attacks, and to be able to defend and enforce its interests

[26] Bundesamt für Sicherheit in der Informationstechnik.

[27] Federal Foreign Office: *Cyber Policy: Multilateral Solutions for the Future.* 25 September 2019.

[28] Cabinet Office: *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World.* November 2011.

more effectively in cyberspace. This presupposes proactive behaviour and active participation in the process of shaping cyberspace, the primary means of which are all peaceful: partly diplomatic and partly economic, as the British Government channels the commercial interests of British companies into the growing international cybersecurity market. The third cyber strategy, re-issued by the British Government on 1 November 2016 for another five years, is a significant step forward.[29] The document sets out three strategic goals – that is why we can call the 2016 cyber strategy the "3D strategy": 'defend, deter and develop' for the realisation of which it considers international action to be essential. In the second of the objectives, cyber diplomacy has a key role to play. Deterrence is envisaged not only by "hard" means (such as developing offensive cyber capabilities) but also by further broadening and deepening cooperation channels – as the strategy states: the British will continue to build on the global cyber alliance that has already begun and continue to support application of international law in cyberspace. Achieving the three strategic goals is only conceivable within an appropriate international framework. The U.K. continues to be at the forefront of creating a free, open, peaceful and secure cyberspace where international law is applicable and fundamental human rights are guaranteed both online and offline. In doing so, the U.K. is counting not only on its traditional allies, but also on its new partners, and is seeking to leverage the power of multilateral fora such as the UN, the G20, the European Union, NATO, the OSCE, the Council of Europe or the British Commonwealth.[30]

Bilateral cyber relations have a key role to play in achieving the goal of building a global cyber alliance. The *United States* is undoubtedly the number one country from among the British traditional allies with which the island nation has had a very close relationship on cyber issues for more than a decade in the context of the so-called "special relationship" – or as it has recently been called "the most important bilateral partnership". The need to involve private sector and business actors, research and development and the application of the basic institutions of the rule of law in cyberspace was already recorded in 2011.[31] In

[29] HM Government: *National Cyber Security Strategy 2016–2021.* United Kingdom, 01 November 2016.

[30] Dóra Molnár: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia [Milestones in the Development of the British Cyber Security I. Establishing the Theoretical Background: The Cyber Security Strategy]. *Hadmérnök,* 12, "KÖFOP" issue (2017). 144.

[31] Cabinet Office: *US–UK Cyber Communiqué.* 25 May 2011.

2015, President Obama and Prime Minister Cameron discussed the details of cooperation in Washington[32] which was finally institutionalised on 7 September 2016 by the cyber agreement signed by the two defence ministers.[33]

Although the U.K. has not yet signed a bilateral agreement with *China,* on 22 October 2015, during the Chinese President's visit to England, the two countries issued a joint statement on building their comprehensive global strategic partnership, launching the "Golden Age" of bilateral relations.[34] As part of this, it was stated that cyber actions aimed at unauthorised theft of intellectual property, trade secrets or confidential business information aimed at gaining a competitive advantage would not be conducted or supported against each other.[35]

Given the special partnership with the United States, it is not surprising that the United Kingdom also established bilateral cyber relations with Japan in 2012. The fifth stop of the biennial meetings was held in Tokyo on 31 January 2020.[36] Opportunities for capacity building and cooperation on the international stage were discussed during the meeting. This is in line with the main areas of cooperation identified at the fourth meeting in 2018, including support for a rules-based international cyber system and the sharing of national solutions for the safe use of IoT devices.[37]

Among the Asian bilateral relations, I would finally like to highlight *India,* which also has huge economic potential for the British – enough to think about the fact that the country already has 600 million Internet users and 650 million mobile users. An important aspect of India–U.K. security cooperation is cyber issues, and the India–U.K. cyber dialogue since 2012 has addressed issues such as cyber risk reduction, cybercrime management and building a global, multilateral, transparent and democratic system of Internet governance. In April 2018, the two countries signed in London a five-year framework agreement of cooperation in

[32] The White House: *Fact Sheet: U.S.–United Kingdom Cybersecurity Cooperation.* Office of the Press Secretary, 16 January 2015.

[33] Terri Moon Cronk: U.S.–U.K. Cyber Agreement Opens Doors for Both Nations. *DoD News,* 08 September 2016.

[34] For more details on some elements of the British China policy see U.K. Parliament: *The Making of UK Strategy towards China.* 04 April 2019.

[35] Foreign and Commonwealth Office: *UK–China Joint Statement 2015.* 22 October 2015.

[36] Ministry of Foreign Affairs of Japan: *The 5th Japan–UK Bilateral Consultations on Cyberspace.* 31 January 2020.

[37] Ministry of Foreign Affairs of Japan: *The 4th Japan–UK Bilateral Consultations on Cyberspace.* 16 March 2018.

14 areas. India has so far only concluded such a comprehensive cyber cooperation agreement with the United States outside the United Kingdom.[38]

The U.K. has already established bilateral cyber relations with a number of European countries. Of these, I highlight the Polish–British cyber cooperation agreement, not primarily because of its content (which is not a significant novelty), but because of its regional significance: through this relationship, the British want to support cyber capacity building programs in Eastern Europe and the Western Balkans.[39]

Finally, with regard to the United Kingdom, we must not forget the *Commonwealth,* which in itself is a long-standing diplomatic forum for the participating states, but in recent years the issue of cybersecurity has also been on the agenda on its own. The participating states institutionalised their cooperation on 20 April 2018 with the signing of the cyber declaration.[40] The declaration reaffirms the obligation of mutual assistance in building cyber capabilities and the need to formulate a common vision for cyberspace, which the U.K. is also financially supporting, contributing £15 million to the stated goals.[41]

Closing Remarks

The cyber preparedness of European states is also outstanding globally. This is well indicated by the Global Cybersecurity Index of the UN International Telecommunication Union (ITU) which provides a ranking of the cyber potential of states. According to the index, the U.K. is the world's leading cyber power, with France in third place. The third state surveyed, Germany, took 26th place.[42] It is very interesting, however, that in the fifth area examined, in terms of cooperation, the English have achieved a very good point, while France, a major diplomatic power, is lagging far behind. However, the examination of cybersecurity in Europe cannot end with a presentation of the three leading European states. There are many refreshing examples of how small countries can achieve great success in

[38] Rahul Roy-Chaudhury: India–UK Cybersecurity Cooperation: The Way Forward. *IISS,* 22 November 2019.

[39] Foreign and Commonwealth Office: *UK–Poland Cyber Co-operation Commitment.* 21 December 2017.

[40] The Commonwealth: *Commonwealth Cyber Declaration.* 20 April 2018.

[41] NCC Group: *Analysis: Untangling the Web of Multi-level Cyber Diplomacy.* 02 May 2018.

[42] UN ITU: *Global Cybersecurity Index 2018.* 2019.

cybersecurity. The index also reflects this, with Lithuania in 4th place and Estonia in 5th place in the overall world ranking. In addition, both states scored higher in the area of cooperation than the three leading major states. This result is a good indication of how small states place emphasis on the importance of cyber diplomacy and see the use of peaceful, diplomatic tools as superior to hard capabilities. In the case of Estonia, for example, it is no exaggeration to say that it has a global leadership role in cybersecurity. The headquarters of NATO and the EU are located in the capital of Estonia, where a number of international cyber arrangements have already been concluded. The small country's guiding role in organisational solutions is also evident: in the autumn of 2019, an independent cyber diplomacy unit was set up in the Ministry of Foreign Affairs, headed by ambassadors, with the task of representing the country in international organisations and fostering bilateral cyber relations – a model worth following.[43] Overall, the European area is at the forefront of the world in all its sub-issues, including cooperation, which could perhaps be the basis for laying the foundations for a peaceful cyberspace.

References

Agence nationale de la sécurité des systèmes d'information: *Défense et sécurité des systèmes d'information. Stratégie de la France.* 2011. Online: www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

Agence nationale de la sécurité des systèmes d'information: *ANSSI/BSI Common Situational Picture.* Vol. 1 – July 2018. Online: www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf

Agence nationale de la sécurité des systèmes d'information: *Second Edition of the Franco–German Common Situational Picture.* 21 May 2019. Online: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F_Reports/Common_Situational_Picture_2019.pdf?__blob=publicationFile&v=2

Burgess, Christopher: Dissecting China's Global Bilateral Cybersecurity Strategy. *Security Boulevard,* 09 October 2016. Online: https://securityboulevard.com/2017/10/dissecting-chinas-global-bilateral-cybersecurity-strategy/

Cabinet Office: *US–UK Cyber Communiqué.* 25 May 2011. Online: www.gov.uk/government/publications/us-uk-cyber-communique

Cabinet Office: *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World.* November 2011. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[43] E-Estonia: *Estonia Takes on a Major Role in Cyber Diplomacy with a New Department for International Cooperation.* 16 October 2019.

Chazan, Guy: German Cyber Security Chief Backs 5G 'No Spy' Deal over Huawei. *Financial Times,* 28 February 2020. Online: www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663

Consulat Général de France á Ekaterinbourg: *La diplomatie française à l'ère numérique.* 29 May 2019. Online: https://ru.ambafrance.org/La-diplomatie-francaise-a-l-ere-numerique

Cronk, Terri Moon: U.S.–U.K. Cyber Agreement Opens Doors for Both Nations. *DoD News,* 08 September 2016. Online: www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/

E-Estonia: *Estonia Takes on a Major Role in Cyber Diplomacy with a New Department for International Cooperation.* 16 October 2019. Online: https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/

Federal Foreign Office: *Cyber Policy: Multilateral Solutions for the Future.* 25 September 2019. Online: www.auswaertiges-amt.de/en/aussenpolitik/themen/multilateralism-cyber/2250332

Federal Ministry of the Interior: *Cyber-Sicherheitsstrategie für Deutschland 2016* [Cybersecurity Strategy for Germany 2016]. Online: www.bmi.bund.de/cybersicherheitsstrategie/BMI_Cyber-SicherheitsStrategie.pdf

Foreign and Commonwealth Office: *UK–China Joint Statement 2015.* 22 October 2015. Online: www.gov.uk/government/news/uk-china-joint-statement-2015

Foreign and Commonwealth Office: *UK–Poland Cyber Co-operation Commitment.* 21 December 2017. Online: www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment

German Institute for International and Security Affairs: *Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016.* Berlin, 11 November 2015. Online: www.swp-berlin.org/en/point-of-view/three-priorities-for-cyber-diplomacy-under-the-german-osce-chairmanship-2016/

HM Government: *National Cyber Security Strategy 2016–2021.* United Kingdom, 01 November 2016. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Laudrain, Arthur P. B.: France's New Offensive Cyber Doctrine. *Lawfare,* 26 February 2019. Online: www.lawfareblog.com/frances-new-offensive-cyber-doctrine

Ministère de l'Europe et des Affaires *Étrangères*: *Appel de Paris pour la confiance et la sécurité dans le cyberespace.* 12 November 2018. Online: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf

Ministère de l'Europe et des Affaires *Étrangères*: *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace. Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018).* Online: www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31.pdf

Ministère de l'Europe et des Affaires Étrangères: *Dinard Declaration on the Cyber Norm Initiative.* 06 April 2019. Online: www.diplomatie.gouv.fr/IMG/pdf/g7_dinard_declaration_on_cyber_initiative_cle4e553d.pdf

Ministère de l'Europe et des Affaires Étrangères: *Indo–French Bilateral Cyber Dialogue (Paris, 20 June 2019).* Online: www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19

Ministère de l'Europe et des Affaires Étrangères: *Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques.* 26 August 2019. Online: www.diplomatie.gouv.fr/IMG/pdf/_fr_synthesis_cyber_norm_initiative_cle025b33.pdf

Ministère de l'Europe et des Affaires Étrangères: *Troisième dialogue stratégique France*–États-*Unis en matière de cybersécurité (Paris, 22 janvier 2020).* Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/actualites-et-evenements-lies-a-la-cybersecurite/article/troisieme-dialogue-strategique-france-etats-unis-en-matiere-de-cybersecurite-22

Ministère de l'Europe et des Affaires *Étrangères*: *La France et la cybersécurité.* s. a. Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/

Ministère des Armées: *Livre Blanc. Défense et sécurité nationale 2013.* Paris. Online: www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf

Ministry of Foreign Affairs of Japan: *The 4th Japan–UK Bilateral Consultations on Cyberspace.* 16 March 2018. Online: www.mofa.go.jp/press/release/press4e_001960.html

Ministry of Foreign Affairs of Japan: *The 5th Japan–UK Bilateral Consultations on Cyberspace.* 31 January 2020. Online: www.mofa.go.jp/press/release/press4e_002766.html

Molnár, Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia [Milestones in the Development of the British Cyber Security I. Establishing the Theoretical Background: The Cyber Security Strategy]. *Hadmérnök,* 12, "KÖFOP" issue (2017). 136–148. Online: http://hadmernok.hu/170kofop_09_molnar.pdf

Nabeel, Fahad: International Cyber Regime: A Comparative Analysis of the US–China–Russia Approaches. *Stratagem,* 1, no. 2 (2018). 8–27. Online: www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_of_the_US-China-Russia_Approaches

NCC Group: *Analysis: Untangling the Web of Multi-level Cyber Diplomacy.* 02 May 2018. Online: www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/nalysis-untangling-the-web-of-multi-level-cyber-diplomacy/

Parameswaran, Prashanth: Singapore–Germany Cyber Cooperation in Focus with Introductory Visit. *The Diplomat,* 14 August 2018. Online: https://thediplomat.com/2018/08/singapore-germany-cyber-cooperation-in-focus-with-introductory-visit/

Rogusky, Przemyslaw: France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I. *Opinio Juris,* 24 September 2019. Online: http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/

Roy-Chaudhury, Rahul: India–UK Cybersecurity Cooperation: The Way Forward. *IISS,* 22 November 2019. Online: www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation

Sénat: *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense.* Par le Sénateur M. Jean-Marie Bockel. Sénat session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012. Online: www.senat.fr/rap/r11-681/r11-6811.pdf

SGDSN: *La stratégie nationale pour la sécurité du numérique.* 2015. Online: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

SGDSN: *Revue stratégique de cyberdéfense*. 12 February 2018. Online: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

The Commonwealth: *Commonwealth Cyber Declaration*. 20 April 2018. Online: https://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf

The White House: *Fact Sheet: U.S.–United Kingdom Cybersecurity Cooperation*. Office of the Press Secretary, 16 January 2015. Online: https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation

U.K. Parliament: *The Making of UK Strategy towards China*. 04 April 2019. Online: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/612/61210.htm

UN ITU: *Global Cybersecurity Index 2018*. 2019. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

U.S. Department of State: *Joint Statement on U.S.–Germany Cyber Bilateral Meeting*. 24 March 2016. Online: https://2009-2017.state.gov/r/pa/prs/ps/2016/03/255082.htm

U.S. Department of State: *Joint Statement on Advancing Responsible State Behavior in Cyberspace*. 23 September 2019. Online: www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/